

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JEFERSON STEVE GONZALEZ ARDILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
POPAYAN CAUCA
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JEFERSON STEVE GONZALEZ ARDILA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL
TÍTULO DE INGENIERO SISTEMAS

DIRECTORA

NANCY GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
POPAYAN CAUCA
2021

NOTA ACEPTACION

Firma Del Presidente Jurado

Firma Del Jurado

Firma Del Jurado

Popayán, 19 octubre 2021

AGRADECIMIENTOS

Me gustaría expresar mi especial agradecimiento primeramente a Dios, por darme la oportunidad de seguir en este diplomado en la academia Cisco Networking, a mi esposa y familia por su motivación y oraciones, a mi universidad por haberme permitido formarme, así como a la directora Nancy Amparo Guaca Professional universitaria, que me apoyo, me ayudo a cruzar este diplomado de profundización de cisco llegando a conocer muchas cosas nuevas. También me gustaría agradecer a mis compañeros que me ayudaron a terminar esta capacitación en el tiempo limitado. Me gustaría extender mi más sincero agradecimiento a cada tutor que nos apoyó en la culminación de este proyecto, quienes ofrecieron muchas sugerencias y colaboración durante la realización de esta formación universitaria y frente a este diplomado atribuyendo a mi formación con su profesionalismo, me encuentro muy agradecido con todos ellos.

CONTENIDO

LISTA DE TABLAS	6
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	11
INTRODUCCIÓN	12
DESARROLLO	13
ESCENARIO 1	13
Aspectos básicos/situación.....	13
Configuraciones básicas.....	14
Paso 1: Configuración básica del R1	14
Paso 2: Configuración básica de switch.....	16
Paso 3: Asignar direcciones IPv4 a los pc	18
ESCENARIO 2.....	22
Paso 1: Inicializar dispositivos.....	22
Paso 2: Configurar R1	29
Paso 3: Configurar R2.....	35
Paso 4: Configurar R3.....	42
Paso 5: Configurar S1	47
Paso 6: Configurar S3.....	49
Paso 7: Verificar la conectividad de la red	51
CONCLUSIONES	90
REFERENCIAS BIBLIOGRÁFICAS.....	91

LISTA DE TABLAS

Tabla 1. Tabla de subnetting VLSM.....	13
Tabla 2. Tabla de direccionamiento.....	13
Tabla 3. Configuración básica de R1.....	18
Tabla 4. Configuración Básica Switch.....	19
Tabla 5. Uso de comandos.....	19
Tabla 6. Configuración del servidor.....	29
Tabla 7. Tareas de configuración R1.....	30
Tabla 8. Tareas de configuración de R2.....	37
Tabla 9. Tareas de configuración R3.....	44
Tabla 10. Tareas de configuración S1.....	48
Tabla 11. Tareas de configuración S3.....	49
Tabla 12. Tabla de verificación de conectividad.....	51
Tabla 13. Tareas de configuración S1, VLAN y routing.....	55
Tabla 14. Tareas de configuración S3.....	58
Tabla 15. Tabla de configuración de R1.....	63
Tabla 16. Tabla Verificación de conectividad de red.....	66
Tabla 17. Tabla de configuración de protocolo OSPF en R1.....	71
Tabla 18. Tabla de configuración de protocolo OSPF en R2.....	72
Tabla 19. Tabla de configuración de OSPF en R2.....	74
Tabla 20. Tabla de verificación de OSPF.....	74
Tabla 21. Tabla de R1 como servidor DHCP.....	78
Tabla 22. Tabla tareas de NAT estática y dinámica R2.....	80
Tabla 23. Tabla de verificación de DHCP y NAT.....	81
Tabla 24. Tabla de configuración NTP.....	83
Tabla 25. Tabla de configuración de listas de acceso.....	85
Tabla 26. Tabla de comando CLI.....	88

LISTA DE FIGURAS

Figura 1. Topología de red escenario 1	13
Figura 2. Topología de red en Packet tracer.....	13
Figura 3. Configuración básica código R1	16
Figura 4. Configuración básica S1	17
Figura 5. Configuración ip a PC A.....	19
Figura 6. Configuración ip a PC B.....	20
Figura 1. Ping a los diferentes dispositivos	20
Figura 8. Topología de red escenario 2	21
Figura 9. Configuración router 1	23
Figura 10. Configuración router 2	24
Figura 11. Configuración router 3	24
Figura 12. Configuración switch 1.....	25
Figura 13. Configuración switch 3.....	26
Figura 14. Verificación base de datos VLAN switch 1.....	27
Figura 15. Verificación base de datos VLAN switch 3.....	28
Figura 16. Inicio de configuración básica R1	30
Figura 17. Configuración básica R1 finalizada.....	31
Figura 18. Configuración de passwords.....	32
Figura 19. Configuración de interfaz	33
Figura 20. Configuración de rutas.....	34
Figura 21. Configuración básica Inicial R2.....	37
Figura 22. Configuración finalizada R2.....	38
Figura 23. Configuración de interfaz 1	39
Figura 24. Configuración de interfaz 2	40

Figura 25. Configuración de interfaz 3	41
Figura 26. Configuración inicial básica R3	43
Figura 27. Configuración R3 en proceso	44
Figura 28. Configuración finalizada de R3	45
Figura 29. Configuración de interfaz en R3	46
Figura 30. Configuración básica S1	47
Figura 31. Configuración básica S3	49
Figura 32. Uso del comando ping R1	51
Figura 33. Configuración comando ping R2	52
Figura 34. Configuración ping R3	53
Figura 35. Switch sin configuración Vlan	55
Figura 36. Switch configuración de Vlan	56
Figura 37. Configuración S3	58
Figura 38. Configuración completa S3	59
Figura 39. Configuración base de datos Vlan	60
Figura 40. Configuración R1	62
Figura 41. Configuración interfaz R1	63
Figura 42. Configuración de conectividad R1	66
Figura 43. Configuración de conectividad S1	67
Figura 44. Configuración de conectividad S3	68
Figura 45. Configuración de conectividad S3 finalizada	69
Figura 46. Configuración de OSPF en R1	70
Figura 47. Configuración OSPF en R2	72
Figura 48. Configuración comando Show ip ospf	74
Figura 49. Configuración comando s hip route ospf	75
Figura 50. Comando show ospf database	76

Figura 51. Configuración de R1 como DHCP	78
Figura 52. Verificación de DHCP	81
Figura 53. Configuración comando Ping a IP 192.168.21.32.....	81
Figura 54. Configuración NTP.....	82
Figura 55. Configuración de NTP en R1.....	83
Figura 56. Verificación acceso remoto R1.....	85
Figura 57. Verificación acceso remoto a R3.....	86
Figura 58. Topología completa escenario.....	87

GLOSARIO

Dirección IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Dirección IP estática: Dirección fija asignada a un equipo o dispositivo conectado a una red.

Enrutador: Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Enrutamiento estático: Reenvío de datos de una red a través de una ruta fija.

IPCONFIG (Internet Protocol Configuration): Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.

Máscara de subred: Código de dirección que determina el tamaño de la red.

Paquete: Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

Ping (Buscador de paquetes de Internet): Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

Topología: Distribución física de una red.

IP: Protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad

Gateways: Dispositivo de una red que sirve como punto de acceso a otra red. El gateway predeterminado es utilizado por un host cuando la dirección de destino de un paquete IP pertenece a algún lugar fuera de la subred local. Un router es un buen ejemplo de un gateway predeterminado.

NVRAM: Memoria de acceso aleatorio no volátil. Memoria de acceso aleatorio que, cuando la computadora se apaga, el contenido de la NVRAM permanece allí.

RESUMEN

En este trabajo se realiza la simulación del primer y segundo escenario propuestos según los requerimientos sugeridos por la guía, construir 2 redes LAN desarrollando el esquema de direccionamiento de cada red, conectado solamente un host a cada red LAN realizando configuraciones básicas a los dispositivos de conexión que son un router y un switch, como asignación de nombre, direcciones IPv4, encriptación de contraseñas, verificación de datos VLAN, también la configuración básica de cada host y por terminal, sustentando la conexión y configuración de cada dispositivo por medio de comandos ping y show.

Palabras clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

In this work, the simulation of the first and second scenario propose, is carried out, according to the requirements suggested by the guide, to build 2 LAN networks, developing the addressing scheme for each network, only one host connected to each LAN network, making basic configurations to the connection devices that are a router and a switch, such as name assignment, IPv4 addresses, password encryption, VLAN verification, also the basic configuration of each host and per terminal, it is necessary to support the connection and configuration of each device by means of ping and show commands.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics

INTRODUCCION

Hoy en día, la tecnología ha avanzado cada vez más y se ha hecho necesario que se implementen actualizaciones dentro de grandes empresas para así fomentar mejores comunicaciones, garantizar la información entre las redes y mejor interconectividad entre diferentes departamentos y áreas dentro de una institución, es por tanto importante garantizar una excelente implementación de un sistema de interconexión que opere de manera ágil y segura, por lo cual, en el presente trabajo se pone a prueba las habilidades aprendidas en el curso de cisco CCNA I yII.

Se considera que el tema más importante de aprender en el desarrollo de este informe es en la aplicación y desarrollo de la técnica subnetting y vlsm, ya que con ese método existen varias maneras de dividir las redes, utilizando fórmulas matemáticas, facilitando el control, la administración y la seguridad de una mega red, al convertirla en subredes, en redes más pequeñas.

En el desarrollo de esta actividad se lleva a cabo el aprendizaje y la puesta en marcha en dividir redes con el protocolo IPv4 e IPv6 utilizando ambas técnicas de subnetting. El restringimiento al acceso del dispositivo es muy importante para la seguridad de cada dispositivo y la conectividad de la red, por lo cual es recomendable siempre agregar el comando que permite cifrar la contraseñas y restringir el acceso a cada dispositivo.

A continuación, el desarrollo de esta actividad de escenario 1 y 2.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología de red escenario 1



Fuente: Guía de actividades

Aspectos básicos/situación

En el desarrollo de este escenario 1, se desenvuelve la topología del caso de estudio, implementando la topología mostrada en la figura 1, configurando el Router R1 y el switch S1, y los Pc. Con las direcciones suministradas en la realización de subnetting y cumpliendo con los requerimientos de LAN1 (100 host) y la LAN2 (50 hosts).

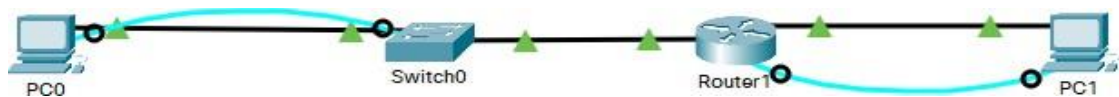
Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Tabla 1. Tabla de subnetting VLSM

LAN	PC S	DIRECCION DE RED	MASCARA	PRIMER IP	ULTIMA IP	BROADCAST	#H
LAN 1	100	192.168.37.0	255.255.255.128	192.168.37.1	192.168.37.126	192.168.37.127	128
LAN 2	50	192.168.37.128	255.255.255.192	192.168.37.129	192.168.37.190	192.168.37.191	64

Fuente: Autoría propia

Figura 2. Topología de red en Packet tracer



Fuente: Autoría propia

Tabla 2. Tabla de direccionamiento

Item	Descripción
Dirección red	192.168.37.0
# host Subred LAN1	100
# host Subred LAN2	50
R1 G0/0/1	192.168.37.1/25
R1 G0/0/0	192.168.37.129/26
S1 SVI	192.168.37.2/25
PC-A	192.168.37.126/25
PC-B	192.168.37.190/26

Fuente: Autoría propia

Configuraciones básicas

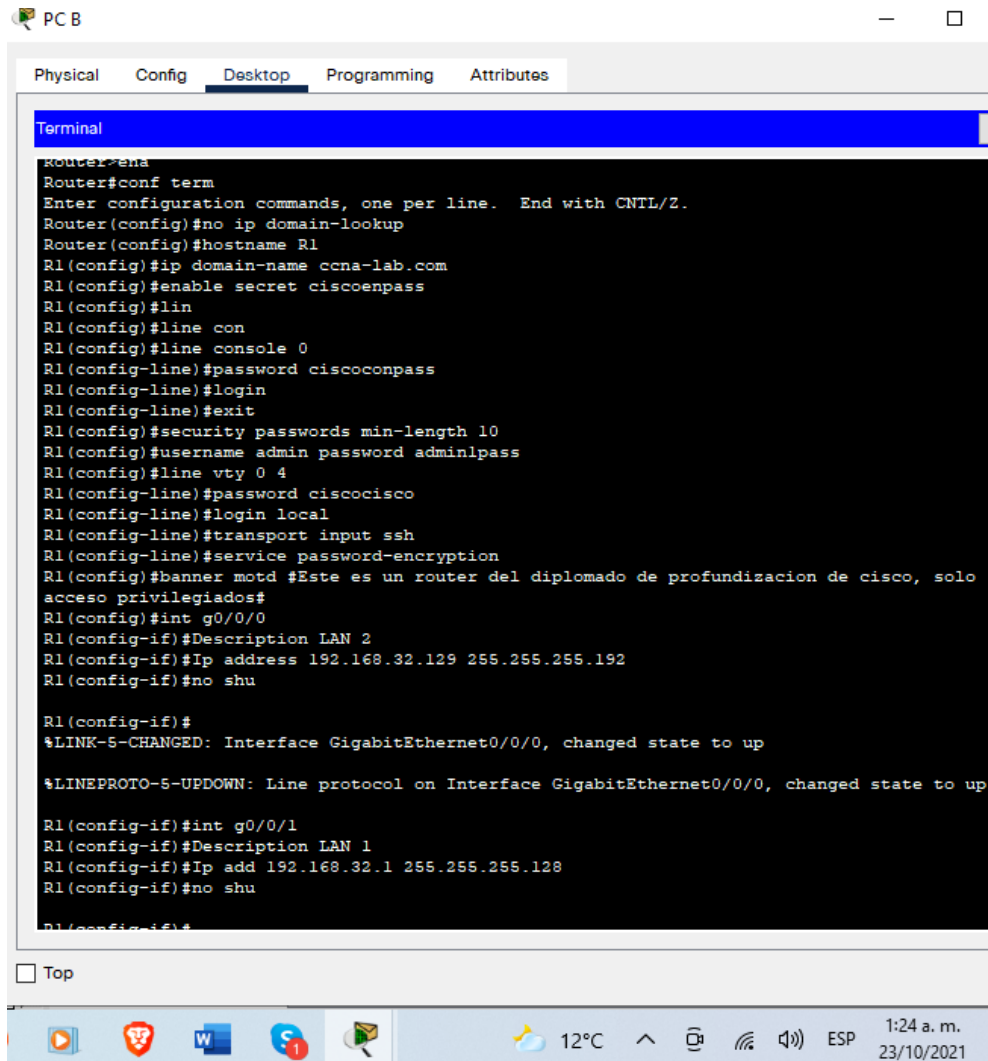
Paso 1: configuración básica del R1

En la tabla 3, se plasma las configuraciones básicas que se le realiza al router 1, comenzando por desactivar la búsqueda DNS, se le asigna el nombre al router (R1), se hace la asignación del dominio ccna-lab.com, se cifra la contraseña para modo EXEC privilegiado y también se establece la contraseña para ingresar a la consola, se establece la longitud mínima de caracteres que es 10, se crea un usuario administrativo en la base de datos local, luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local esta VTY, se configura para que solo acepte SSH, se cifran las contraseñas de texto no cifrado, se hace la configuración de un MOTD Banner con su respectivo mensaje de alerta y por último se agrega direcciones IPv4 a las interfaz G0/0/0 Y G0/0/1

Router(config)#no ip domain-lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	cambiar nombre del router
R1(config)#ip domain-name ccna-lab.com	asignar nombre de dominio
R1(config)#enable secret ciscoenpass	Contraseña cifrada para el modo EXEC privilegiado
R1(config)#line console 0	cambiar la contraseña al acceso de consola
R1(config-line) #password ciscoenpass	
R1(config-line)#login	
R1(config)#security passwords min-length 10	Establecer la longitud mínima para las contraseñas 10 caracteres
R1(config)#username admin password admin1pass	Crear un usuario

	administrativo en la base de datos local
R1(config)#line vty 0 4	Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#password cisco	
R1(config-line)#login local	
R1(config-line)#transport input ssh	Configurar VTY solo aceptando SSH
R1(config-line)#service password-encryption	Cifrar las contraseñas de texto no cifrado
R1(config)#banner motd #Este es un router del diplomado de profundización de cisco, solo accesos privilegiados#	Configurar un MOTD Banner
R1(config)#int g0/0/0	Acceder a la Interfaz
R1(config-if)#Description LAN 2	Agrega description
R1(config-if)#ip address 192.168.37.129 255.255.255.192	Asignar dirección ip
R1(config-if)#no shu	Encender Interfaz
R1(config-if)#int g0/0/1	Acceder a la Interfaz
R1(config-if)#Description LAN 1	description
R1(config-if)#ip add 192.168.37.1 255.255.255.128	Asignar dirección ip
R1(config-if)#no shu	Encender Interfaz
R1(config)#crypto key generate rsa	Generar una clave de cifrado RSA
How many bits in the modulus [512]: 1024	

Figura 3. Configuración Básica código R1



```
router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#lin
R1(config)#line con
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin password adminpass
R1(config)#line vty 0 4
R1(config-line)#password ciscocisco
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#service password-encryption
R1(config)#banner motd #Este es un router del diplomado de profundizacion de cisco, solo
acceso privilegiados#
R1(config)#int g0/0/0
R1(config-if)#Description LAN 2
R1(config-if)#Ip address 192.168.32.129 255.255.255.192
R1(config-if)#no shu

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#int g0/0/1
R1(config-if)#Description LAN 1
R1(config-if)#Ip add 192.168.32.1 255.255.255.128
R1(config-if)#no shu
R1(config-if)#
```

Fuente: Autoría propia

Paso 2 configuración básica de switch

En este paso se realiza una configuración básica de switch, como la parte de la seguridad del dispositivo, agregando contraseña al modo consola y al modo EXEC privilegiado, encriptación y cifrado de textos, desactivación de búsqueda DNS, se crea un usuario en la base de datos local con su contraseña, se configuran para que solo acepte SSH, se configura la interfaz de administración SVI y se realiza la configuración del Gateway predeterminado.

Configuración S1

Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNS.
Switch(config)#host S1	Nombre del switch
S1(config)#ip domain-name ccna-lab.com	Nombre de dominio
S1(config)#Enable secret ciscoenpass	Contraseña cifrada para el modo EXEC privilegiado
S1(config)#Line console 0	Contraseña de acceso a la consola
S1(config-line)#Password ciscoconpass	
S1(config-line)#login	
S1(config)#username admin password admin1pass	Crear un usuario administrativo en la base de datos local
S1(config)#Line vty 0 15	Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
S1(config-line)#Password cisco	
S1(config-line)#Login local	
S1(config-line)#transport input ssh	Configurar las líneas VTY para que acepten únicamente las conexiones SSH
S1(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
S1(config)#Banner motd #Este es un switch del diplomado de profundización de cisco, solo acceso a privilegiados#	Configurar un MOTD Banner
S1(config)#crypto key generate rsa	Generar una clave de cifrado RSA
How many bits in the modulus [512]: 1024	
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	
S1(config)#Int vlan 1	Configurar la interfaz de administración (SVI)
S1(config-if)#Ip add 192.168.37.2 255.255.255.128	
S1(config-if)#no shut	
S1(config-if)#Ip default-gateway 192.168.37.1	Configuración del gateway predeterminado

Figura 4. Configuración básica S1

```

Switch>ena
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#Enable secret ciscoenpass
S1(config)#Line console 0
S1(config-line)#Password ciscoconpass
S1(config-line)#LOGIN
S1(config-line)#username admin password adminlpass
S1(config)#username admin password adminlpass
S1(config)#Line vty 0 15
S1(config-line)#Password ciscocisco
S1(config-line)#Login local
S1(config-line)#exit
S1(config)#transport input ssh
^
% Invalid input detected at '^' marker.

S1(config)#transport input ssh
^
% Invalid input detected at '^' marker.

S1(config)#tra
S1(config)#tra?
% Unrecognized command
S1(config)#lin
S1(config)#line vt
S1(config)#line vty 0 15
S1(config-line)#tra
S1(config-line)#transport inp
S1(config-line)#transport input ssh
    
```

Fuente: Autoría propia

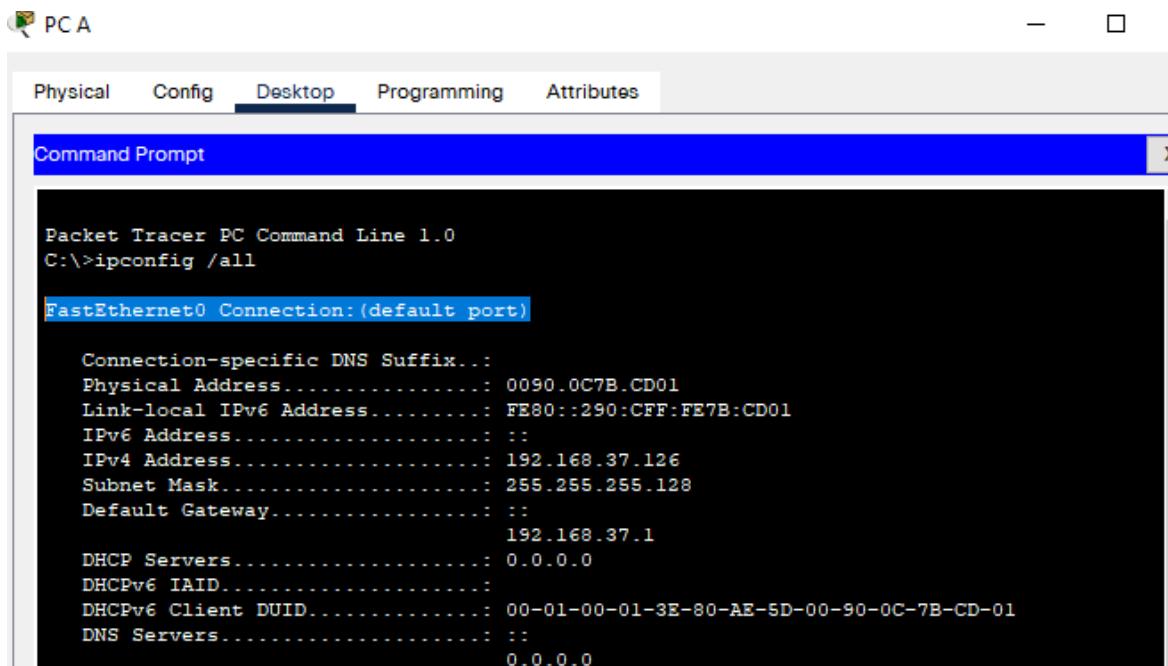
Paso 3 Asignar direcciones IPv4 a los pc

Tabla 3. Descripción de Dirección ip PC – A

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0090.0C7B.CD01
Dirección IP	192.168.37.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.37.1

Fuente: Autoría propia

Figura 5. Configuración ip a PC A



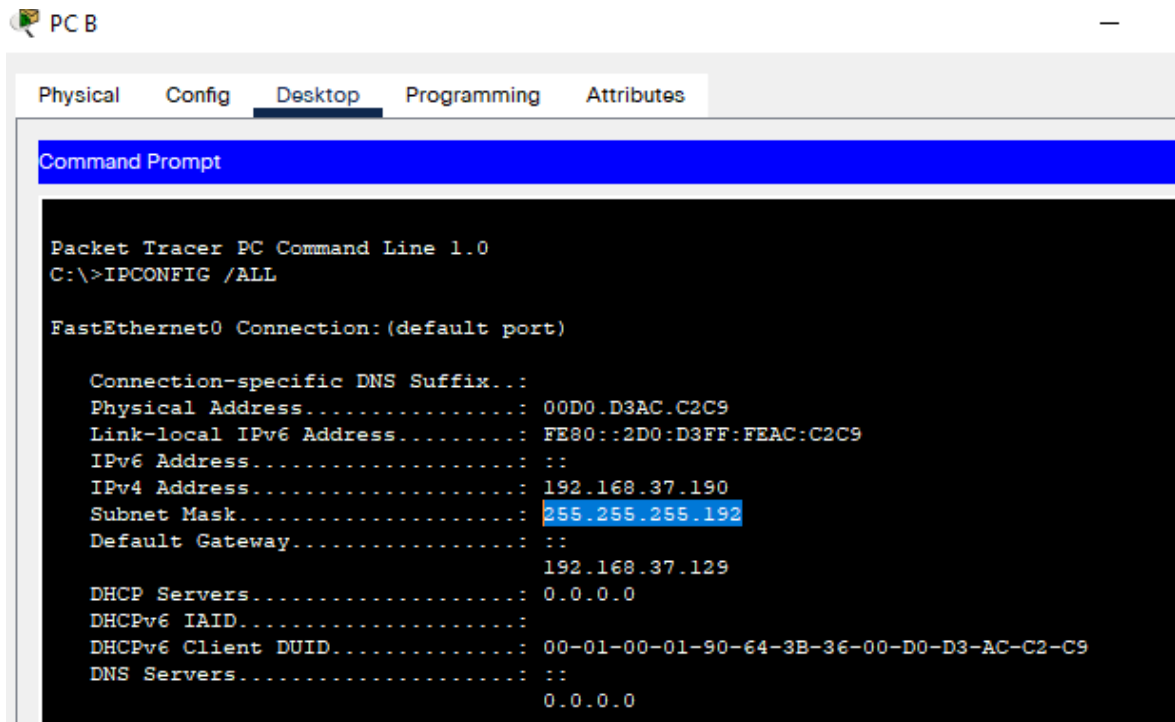
Fuente: Autoría propia

Tabla 4. Descripción de Dirección ip PC – B

PC-B Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	00D0.D3AC.C2C9
Dirección IP	192.168.37.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.37.129

Fuente: Autoría propia

Figura 6. Configuración ip a PC B



The image shows a screenshot of the Packet Tracer interface for PC B. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the 'IPCONFIG /ALL' command, resulting in the following configuration details for the FastEthernet0 interface:

```
Packet Tracer PC Command Line 1.0
C:\>IPCONFIG /ALL

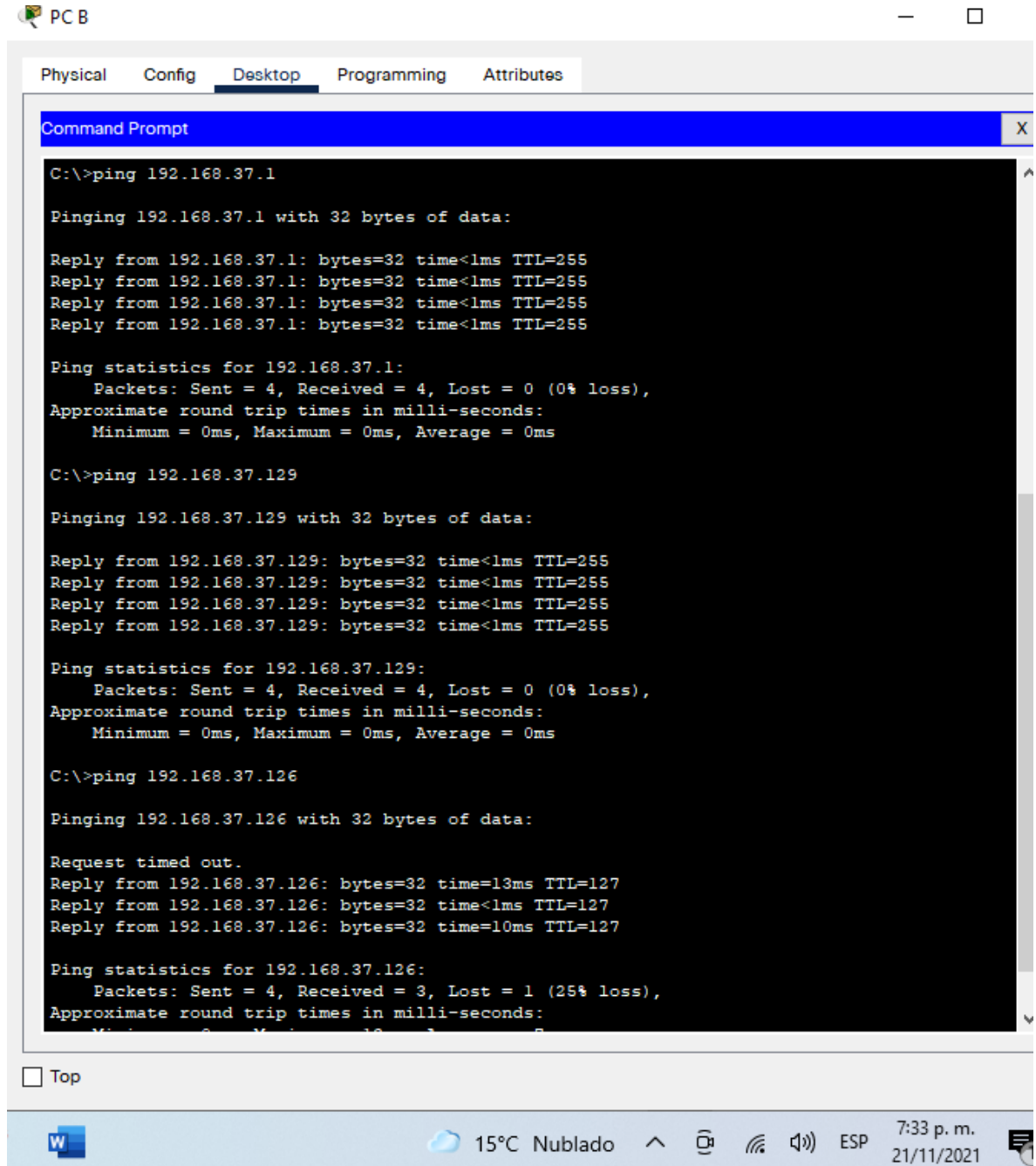
FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address..... : 00D0.D3AC.C2C9
Link-local IPv6 Address..... : FE80::2D0:D3FF:FEAC:C2C9
IPv6 Address..... : ::
IPv4 Address..... : 192.168.37.190
Subnet Mask..... : 255.255.255.192
Default Gateway..... : ::
                               192.168.37.129
DHCP Servers..... : 0.0.0.0
DHCPv6 IAID..... :
DHCPv6 Client DUID..... : 00-01-00-01-90-64-3B-36-00-D0-D3-AC-C2-C9
DNS Servers..... : ::
                               0.0.0.0
```

Fuente: Autoría propia

Paso 4 Verificación de conexión y configuración.

Figura 7. Ping a los diferentes dispositivos



```
PC B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.37.1

Pinging 192.168.37.1 with 32 bytes of data:

Reply from 192.168.37.1: bytes=32 time<lms TTL=255
Reply from 192.168.37.1: bytes=32 time<lms TTL=255
Reply from 192.168.37.1: bytes=32 time<lms TTL=255
Reply from 192.168.37.1: bytes=32 time<lms TTL=255

Ping statistics for 192.168.37.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.37.129

Pinging 192.168.37.129 with 32 bytes of data:

Reply from 192.168.37.129: bytes=32 time<lms TTL=255
Reply from 192.168.37.129: bytes=32 time<lms TTL=255
Reply from 192.168.37.129: bytes=32 time<lms TTL=255
Reply from 192.168.37.129: bytes=32 time<lms TTL=255

Ping statistics for 192.168.37.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.37.126

Pinging 192.168.37.126 with 32 bytes of data:

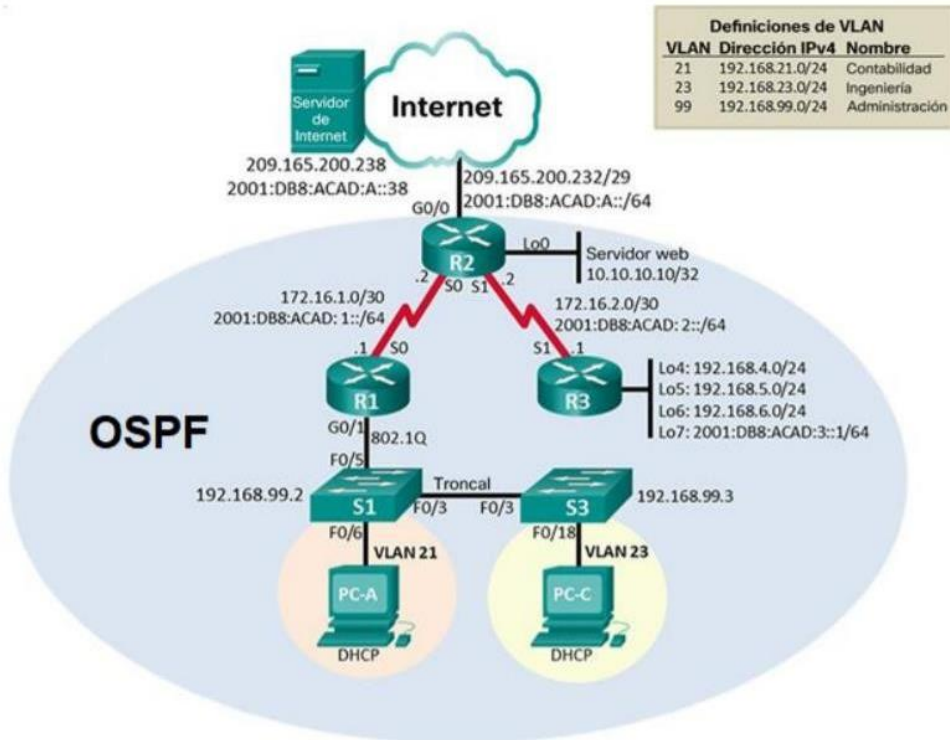
Request timed out.
Reply from 192.168.37.126: bytes=32 time=13ms TTL=127
Reply from 192.168.37.126: bytes=32 time<lms TTL=127
Reply from 192.168.37.126: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.37.126:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
```

Fuente: Autoría propia

2. ESCENARIO 2 Topología

Figura 8. Topología de red escenario 2



Fuente: Guía de actividades

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches.

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Comandos para usar

- Erase startup-config.
- Reload.

Tabla 5. Uso de comandos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>en Router#erase Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>en Switch#sh flash Directory of flash:/ 1 -rw- 3058048 <no date> c2950-i6q4l2-mz.121-22.EA4.bin 64016384 bytes total (60958336 bytes free) Switch# Switch#

Fuente: Autoría propia

Figura 9. Configuración router 1

The image shows a network simulation interface. On the left, a network diagram features three routers: Router1 (top), Router2 (middle), and Router3 (bottom right). Router1 is connected to Router2 via S0/1/0 and S0/1/1. Router2 is connected to Router3 via S0/1/0 and S0/1/1. A server labeled 'Server-PT SERVIDOR WEB' is connected to Router3. A table titled 'Definición de VLAN' is visible:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

Below the diagram, a 'Troncal' link is shown between two switches, with IP address 192.168.99.3 and interface Fa0/18. A 'VLAN 23' is also indicated. On the right, a 'CLI' window for 'Router1' displays the following text:

```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#erase
Router#
Router#
Router#erase st
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]OK!
Erase of nvram: complete
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
Router#reload
Proceed with reload? [confirm]Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

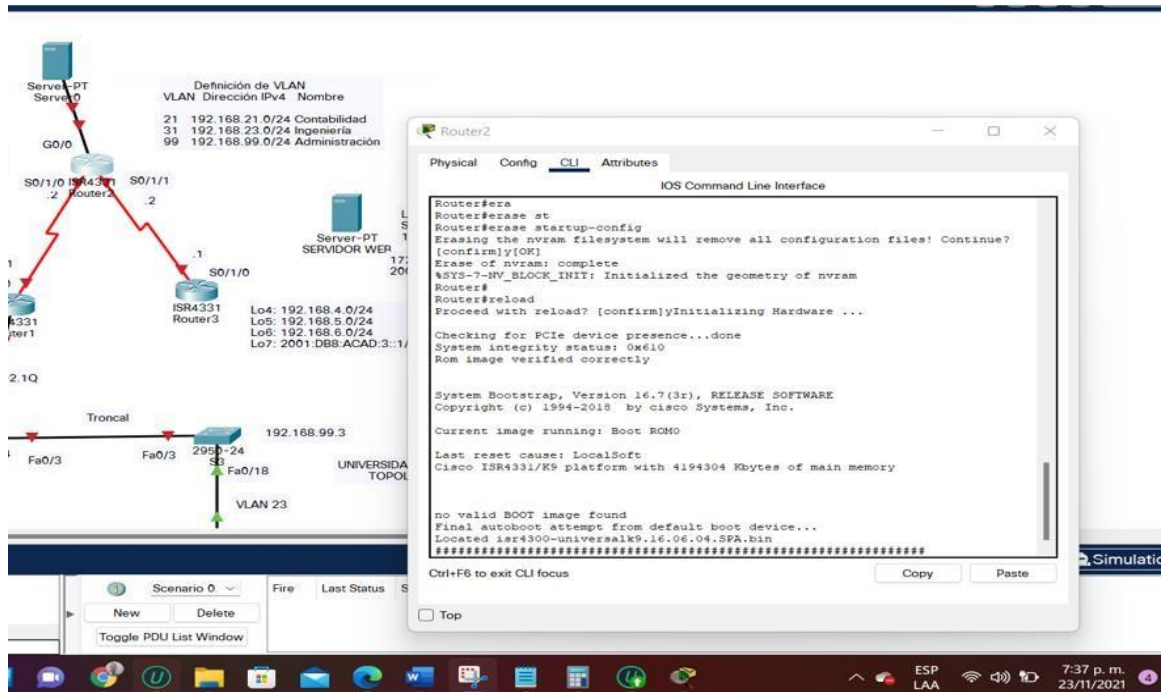
Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory
  
```

The bottom of the screenshot shows a Windows taskbar with the time 7:36 p.m. on 23/11/2021.

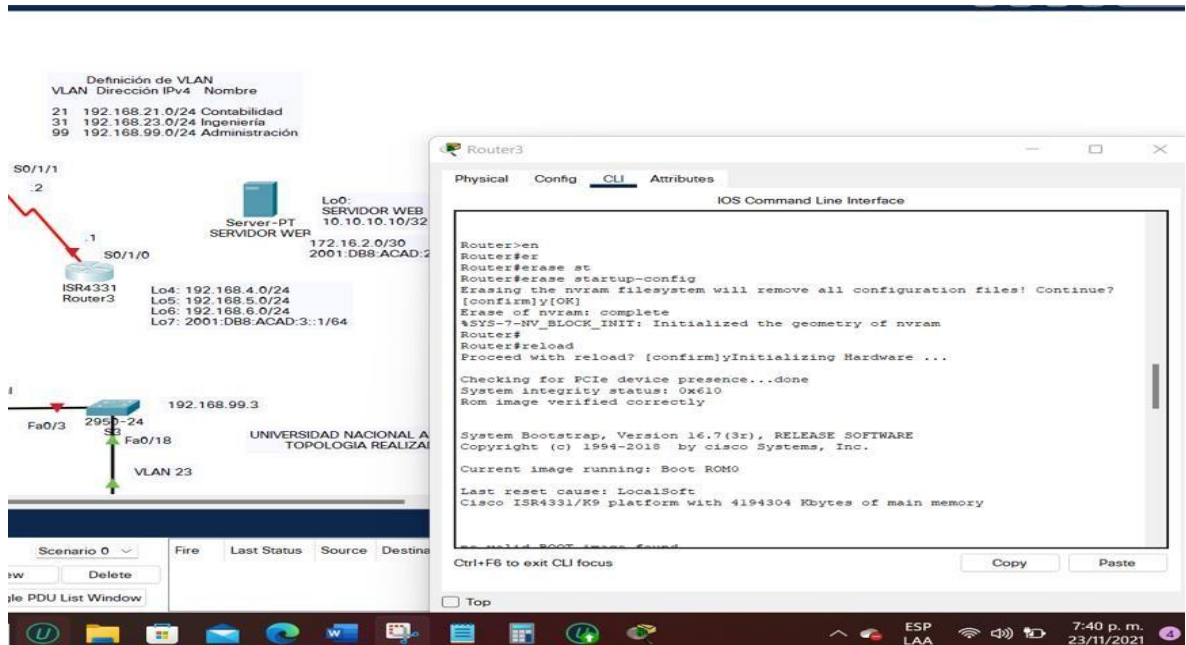
Fuente: Autoría propia

Figura 10. Configuración router 2



Fuente: Autoría propia

Figura 11. Configuración router 3



Fuente: Autoría propia

Figura 12. Configuración switch 1

The image displays a network configuration environment. On the left, a network diagram shows an ISR4331 Router3 connected to a Server-PT (SERVIDOR WEB) and a switch (2950-24 S3). The switch is connected to a PC (192.168.99.3) via Fa0/18. The switch is configured with VLAN 23. The router has interfaces S0/1/0 and S0/1/1. The server has IP 172.16.2.0/30. The PC has IP 192.168.99.3. The switch has IP 192.168.99.3. The switch is connected to the router via S0/1/0.

Definición de VLAN

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

Lo0: SERVIDOR WEB 10.10.10.10/32
172.16.2.0/30 2001:DB8:ACAD:2

Lo4: 192.168.4.0/24
Lo5: 192.168.5.0/24
Lo6: 192.168.6.0/24
Lo7: 2001:DB8:ACAD:3::1/64

192.168.99.3

UNIVERSIDAD NACIONAL AGRARIA LA ROSA
TOPOLOGIA REALIZADA

Scenario 0

New Delete

toggle PDU List Window

IOS Command Line Interface

```
state to up
Switch>en
Switch#er
Switch#erase st
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
Switch#re
Switch#rel
Switch#reload
Proceed with reload? [confirm]yC2950 Boot Loader (C2950-HBOOT-M) Version
12.1(11r)EAL, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by miwang
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of
memory.
2950-24 starting...
Base ethernet MAC Address: 000C.CF9A.6A4A
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 3058048
flashfs[0]: Bytes available: 60958336
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Ctrl+F6 to exit CLI focus
```

7:42 p. m.
23/11/2021

Fuente: Autoría propia

Figura 13. Configuración switch 3

The image shows a network configuration interface with three main components:

- VLAN Definition Table:**

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración
- Network Diagram:** Shows an ISR4331 Router3 connected to a Server-PT (SERVIDOR WEB) and a switch. The switch has Fa0/3 connected to 2950-24 and Fa0/18 connected to VLAN 23. IP addresses for the switch include 192.168.99.3.
- CLI Window (S3):** Shows the following commands and output:

```
Switch>
Switch>en
Switch#er
Switch#erase at
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
Switch#rel
Switch#reload
Proceed with reload? [confirm]yC2950 Boot Loader (C2950-HBOOT-M) Version
12.1(11r)EAL, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by miwang
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of
memory.
2950-24 starting...
Base ethernet MAC Address: 0006.2ACA.8022
Xmodem file system is available.
Initializing Flash...
flashfs(0): 1 files, 0 directories
flashfs(0): 0 orphaned files, 0 orphaned directories
flashfs(0): Total bytes: 64016384
flashfs(0): Bytes used: 3058048
flashfs(0): Bytes available: 60958336
flashfs(0): flashfs fsck took 1 seconds.
...done Initializing Flash.
```

Fuente: Autoría propia

Figura 14. Verificación base de datos VLAN switch 1

The screenshot displays a network simulation interface. On the left, a network diagram shows a central switch (UNIVERSID TOP) connected to three routers (ISR4331 Router1, Router2, Router3) and a server (Server-PT SERVIDOR WER). The switch is configured with VLAN 23. A table titled 'Definición de VLAN' lists the following:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

Below the table, the switch configuration for VLAN 23 is shown:

```
Lo4: 192.168.4.0/24
Lo5: 192.168.5.0/24
Lo6: 192.168.6.0/24
Lo7: 2001.DBB.ACAD.3...
```

The main window shows the CLI of a switch (S1) in the 'CLI' tab. The output of the 'show flash' command is as follows:

```
IOS Command Line Interface
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHR0610Z0WC
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed
state to up

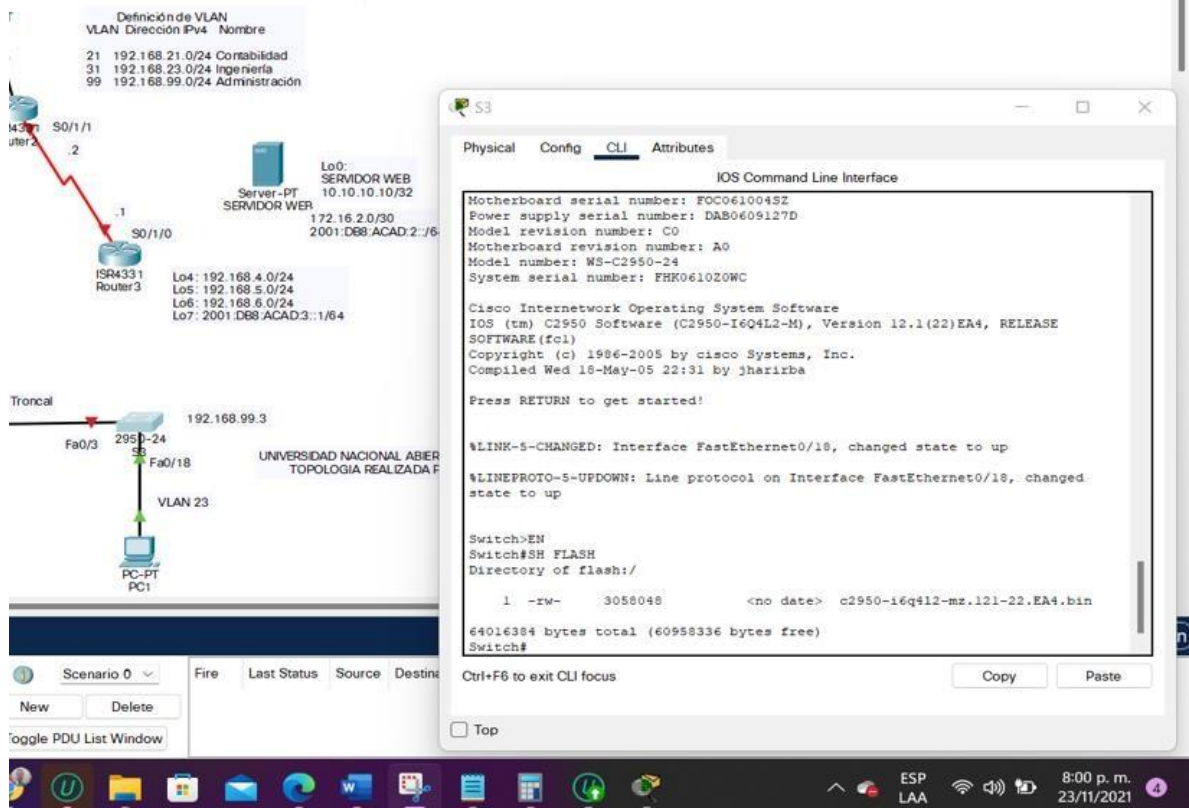
Switch>en
Switch#sh flash
Directory of flash:/

 1  -rw-   3058048      <no date>  c2950-16q4l2-mz.121-22.EA4.bin

64016384 bytes total (60958336 bytes free)
Switch#
Switch#
Switch#
```

Fuente: Autoría propia

Figura 15. Verificación base de datos VLAN switch 3



Fuente: Autoría propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 6. Configuración del servidor

Elemento o tarea a configurar	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autoría propia

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7. Tareas de configuración R1

Elemento o tarea a configurar	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/1/0	R1(config)#interface serial 0/1/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R1(config)#ipv6 route ::/0 s0/1/0 R1(config)#ipv6 uni R1(config)#ipv6 unicast-routing R1(config)#

Fuente: Autoría propia

Figura 16. Inicio de configuración básica R1

The image shows a network simulator interface. On the left, a network diagram features a central Router2 connected to a Server-PT (Server0) via its G0/0 interface. Router2 is also connected to Router1 and Router3 via its S0/1/0 and S0/1/1 interfaces. Router1 is connected to a PC-PT (PC1) via its Fa0/24 interface. A 'Troncal' link is shown between Router2 and Router3. A table titled 'Definición de VLAN' is visible, listing VLANs 21, 31, and 99 with their respective IPv4 addresses (192.168.x.x).

Overlaid on the right is the 'Router1' CLI window. The window title is 'Router1' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface' and displays the following text:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable pass
Router(config)#enable password cisco
Router(config)#enable password class
Router(config)#!l
Router(config)#!l
Router(config)#line con 0
Router(config-line)#pas
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#serv
Router(config)#service pas
Router(config)#service password-encryption
Router(config)#ba
Router(config)#banner mo
Router(config)#banner motd #Se prohíbe el acceso no autorizado#
Router(config)#
```

At the bottom of the CLI window, there are buttons for 'Copy' and 'Paste', and a 'Top' button. The Windows taskbar at the bottom shows the time as 8:24 p.m. on 23/11/2021.

Fuente: Autoría propia

Figura 17. Configuración básica R1 finalizada

The image shows a network simulator interface. On the left, a network diagram displays three routers: Router1 (ISR4331), Router2 (ISR4331), and Router3 (ISR4331). Router1 is connected to Router2 via S0/1/0 and S0/1/1. Router2 is connected to Router3 via S0/1/1 and S0/1/0. A server (Server-PT) is connected to Router2 via G0/0. A PC (PC-PT) is connected to Router3 via Fa0/24. A trunk link connects Router1 (Fa0/24) and Router3 (Fa0/24). A table titled 'Definición de VLAN' is visible, listing VLANs 21, 31, and 99 with their respective IPv4 addresses (192.168.21.0, 192.168.31.0, 192.168.99.0).

The main window shows the CLI configuration for Router1:

```
Router1
Router1>en
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#no ip domain-lookup
Router1(config)#enable pass
Router1(config)#enable password cisco
Router1(config)#enable password class
Router1(config)#!l1
Router1(config)#!l1
Router1(config)#line con 0
Router1(config-line)#pas
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#serv
Router1(config)#service pas
Router1(config)#service password-encryption
Router1(config)#ba
Router1(config)#banner mo
Router1(config)#banner motd #Se prohíbe el acceso no autorizado#
Router1(config)#
Router1(config)#hostg
Router1(config)#host
Router1(config)#hostname R1
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#pass
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#
```

The bottom of the image shows a Windows taskbar with the system clock at 8:35 p. m. on 23/11/2021.

Fuente: Autoría propia

Figura 18. Configuración de passwords

The screenshot displays a network simulation environment. On the left, a network diagram shows three routers: Router1 (ISR4331), Router2 (ISR4331), and Router3 (ISR4331). Router1 is connected to Router2 and Router3. Router2 is connected to a server (Serve-PT) and a PC (PC1). Router3 is connected to a PC (PC1). A table titled 'Definición de VLAN' is visible in the background:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	
31	192.168.23.0/24	
99	192.168.99.0/24	

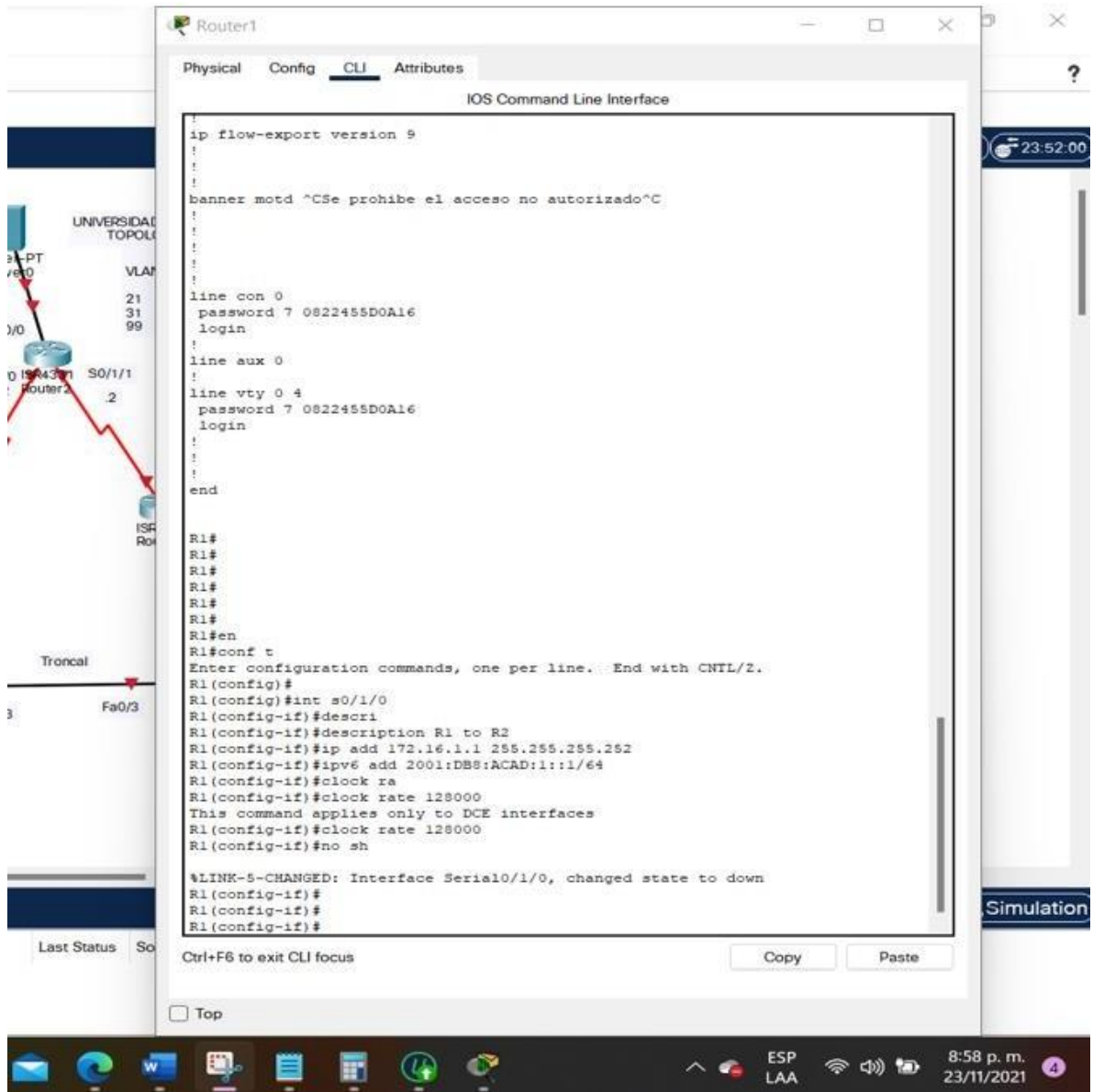
On the right, the CLI window for Router1 shows the following configuration:

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
clock rate 2000000
shutdown
?
interface Vlan1
no ip address
shutdown
?
ip classless
?
ip flow-export version 9
?
?
?
?
banner motd ^CSe prohíbe el acceso no autorizado^C
?
?
?
?
?
?
?
line con 0
password 7 0822455D0A16
login
?
line aux 0
?
?
line vty 0 4
password 7 0822455D0A16
login
?
?
?
?
end

Ctrl+F6 to exit CLI focus
Copy Paste
 Top
```

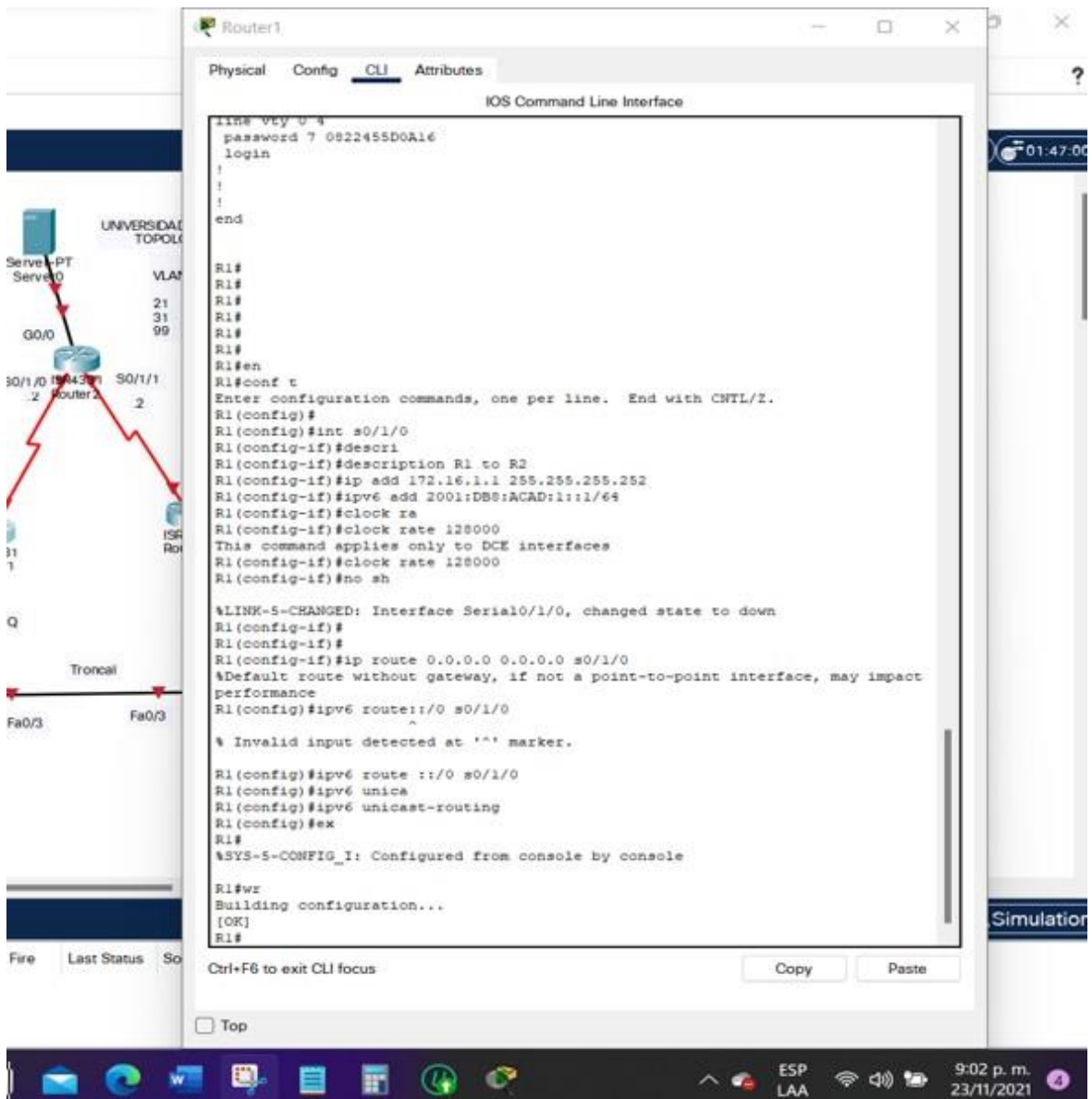
Fuente: Autoría propia

Figura 19. Configuración de interfaz



Fuente: Autoría propia

Figura 20. Configuración de rutas



Fuente: Autoría propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2.

La configuración del R2 incluye las siguientes tareas:

Tabla 8. Tareas de configuración de R2

Elemento o tarea para configurar	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup

Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/1/0	R2(config)#interface serial 0/1/0 R2(config-if)#description R1 to R2 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz S0/1/1	R2(config)#interface serial 0/1/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit

Interfaz G0/0/0 (simulación de Internet)	<pre> R2(config)#interface gigabitEthernet 0/0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/6 4 R2(config-if)#no shutdown R2(config- if)# R2(config-if)#exit </pre>
Interfaz loopback 0 (servidor web simulado)	<pre> R2(config)#interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit </pre>

Fuente: Autoría propia

Figura 21. Configuración básica Inicial R2

The image shows a network simulator interface. On the left, a network diagram includes a server labeled 'Server0', a central router 'Router2', and another router 'Router3'. A table titled 'Definición de VLAN' is visible in the background:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	

The main focus is the 'Router2' CLI window, which displays the following configuration commands:

```
Router>en
Router#no ip dom
Router#no ip domain-lookup
^
Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ena
Router(config)#enable pass
Router(config)#enable password class
Router(config)#line con 0
Router(config-line)#passw
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#serv
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#ban
Router(config)#banner motd
Router(config)#banner motd #5e prohíbe el acceso no autorizado#
Router(config)#
```

The bottom of the image shows a Windows taskbar with the system clock indicating 8:27 p.m. on 23/01/2021.

Fuente: Autoría propia

Figura 22. Configuración finalizada R2

The image shows a network configuration interface. On the left, a network diagram includes a switch (ISR4331) and two routers (Router2 and Router3). A red arrow points from Router2 to Router3. A table titled 'Definición de VLAN' is visible:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.21.0/24	

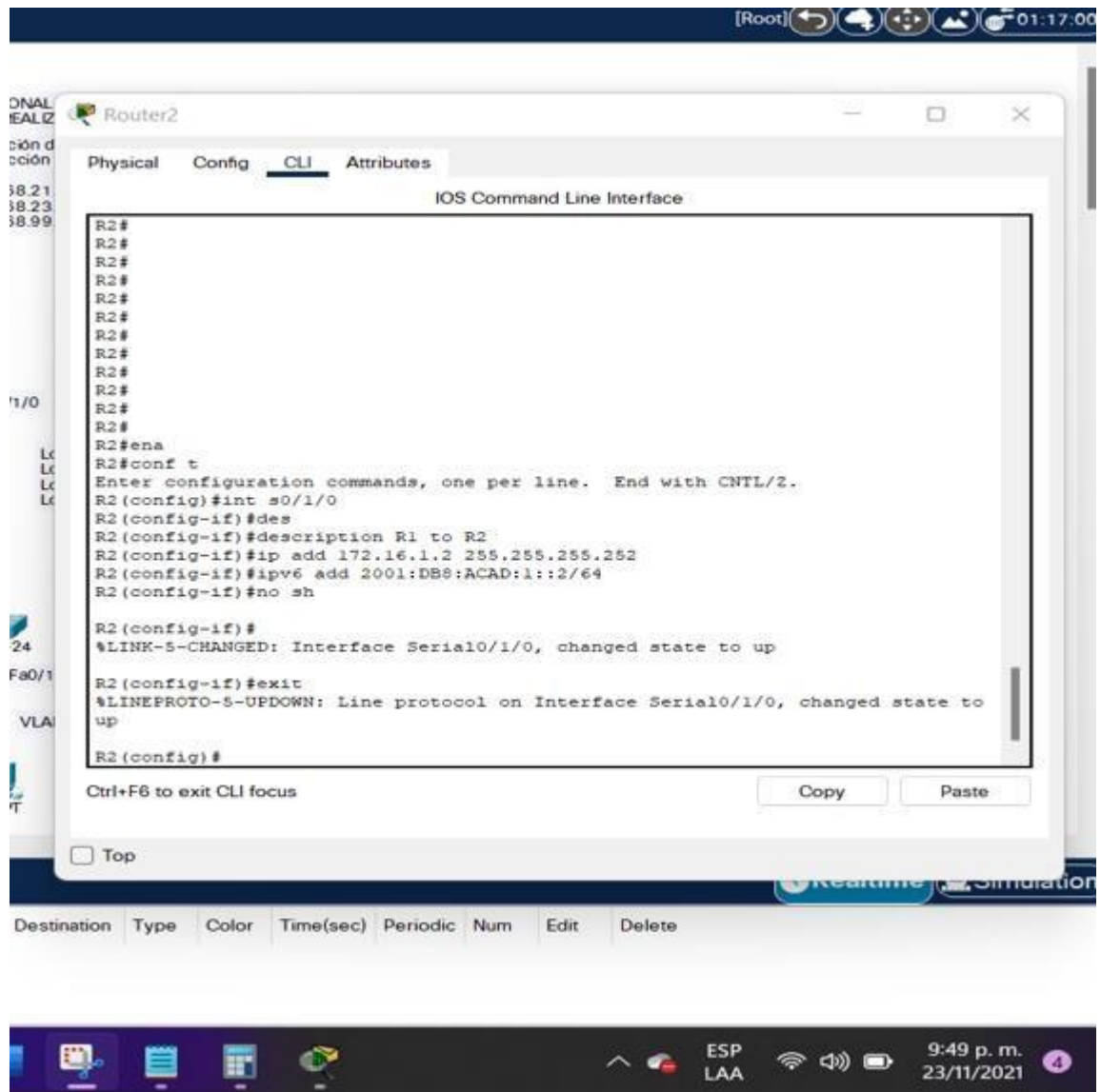
The main window displays the 'IOS Command Line Interface' for Router2. The configuration commands are as follows:

```
Router(config)#no ip domain-lookup
Router(config)#ena
Router(config)#enable pass
Router(config)#enable password class
Router(config)#line con 0
Router(config-line)#passw
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#serv
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#ban
Router(config)#banner mot
Router(config)#banner motd #Se prohíbe el acceso no autorizado#
Router(config)#
Router(config)#
Router(config)#
Router(config)#host
Router(config)#hostname
% Incomplete command.
Router(config)#hostname R2
R2(config)#
R2(config)#line vty 0 4
R2(config-line)#pass
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

The interface also shows a 'Troncal' link between Fa0/3 and 2951, and a 'PC' icon. The system tray at the bottom indicates the time is 8:36 p. m. on 23/11/2021.

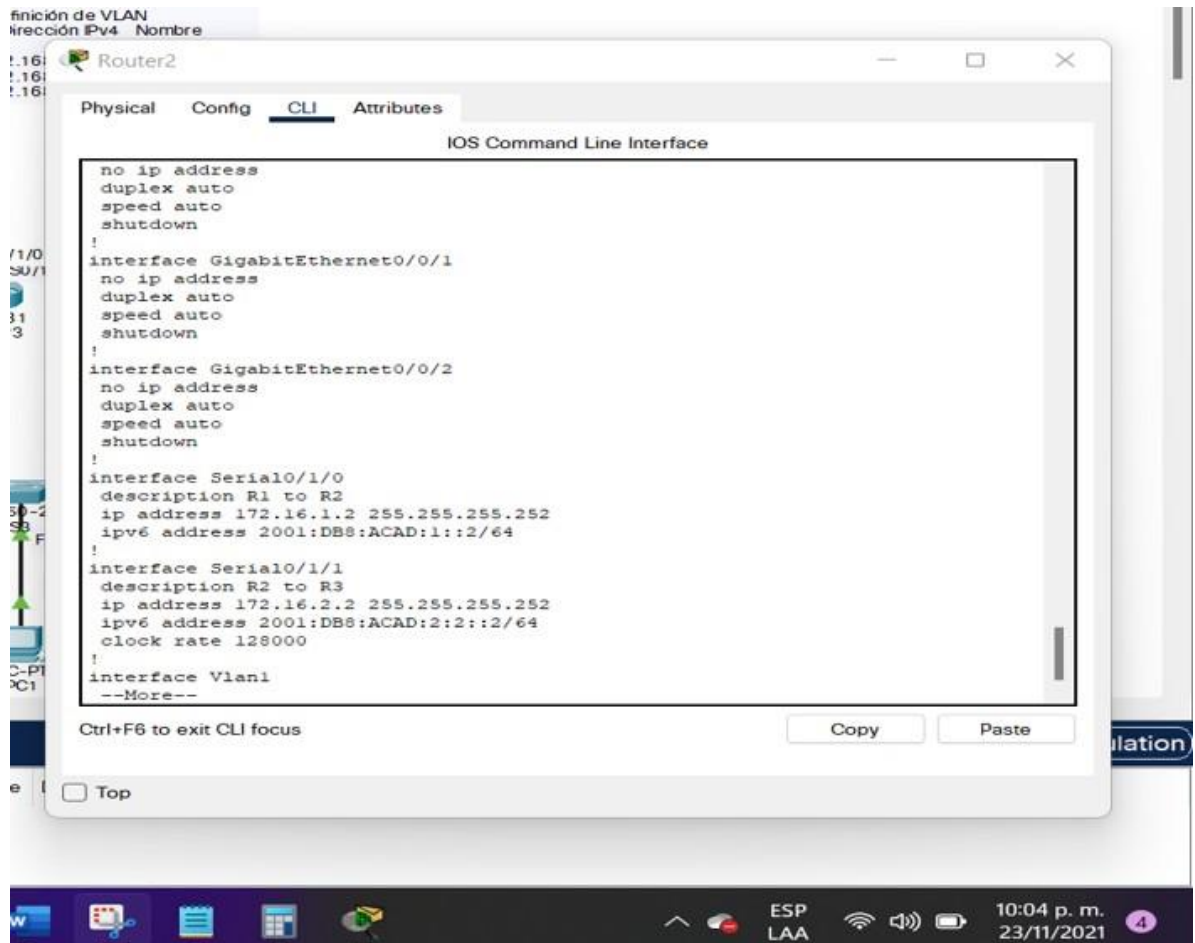
Fuente: Autoría propia

Figura 23. Configuración de interfaz 1



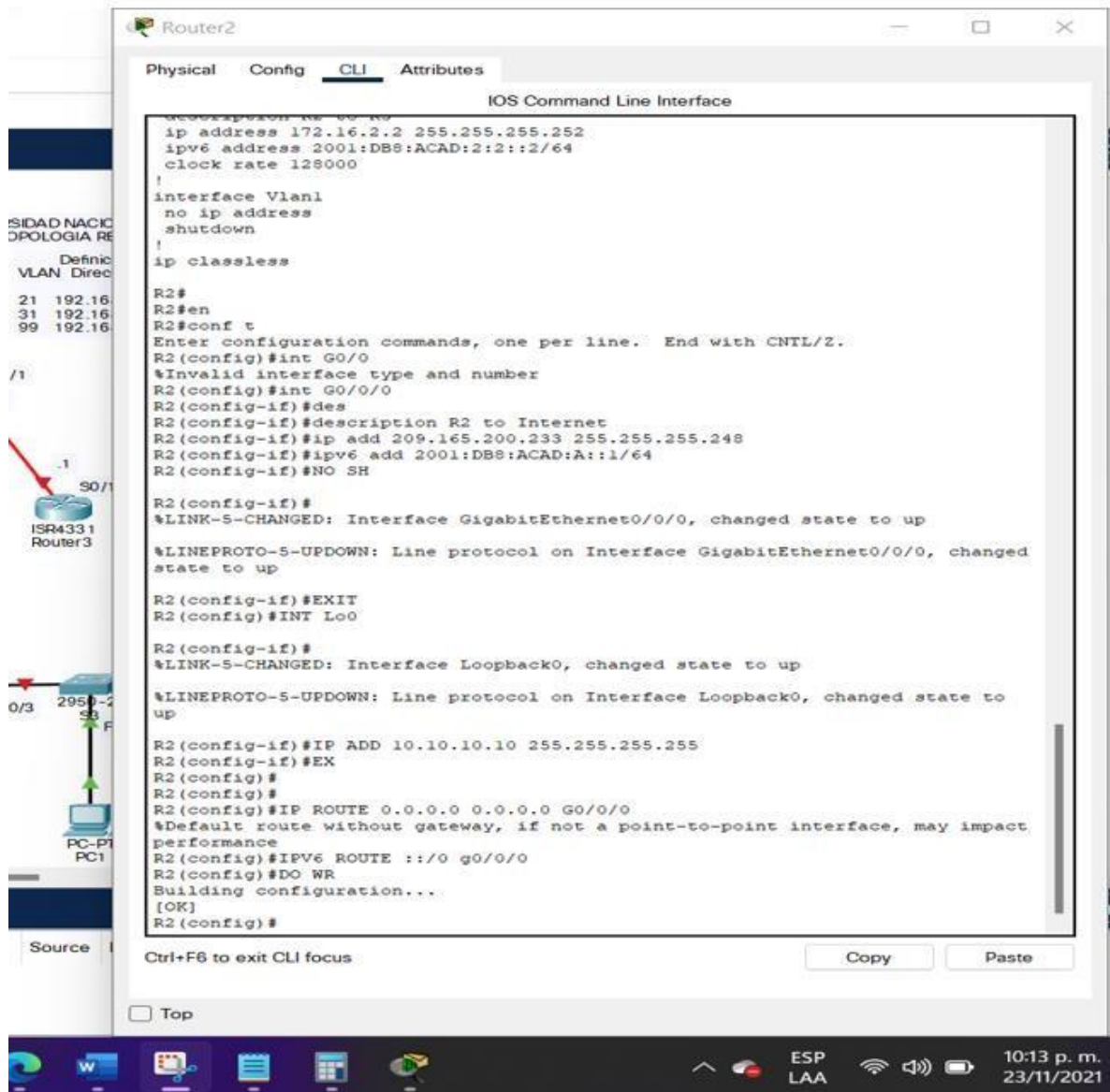
Fuente: Autoría propia

Figura 24. Configuración de interfaz 2



Fuente: Autoría propia

Figura 25. Configuración de interfaz 3



Fuente: Autoría propia

Paso 4: Configurar R3 La configuración del R3 incluye las siguientes tareas:

Tabla 9. Tareas de configuración R3

Elemento o tarea a configurar	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3

Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/1/0	R3(config)#interface serial 0/1/0 R3(config-if)#description R3 a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)# R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit.
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#

Rutas predeterminadas

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0  
R3(config)#ipv6 route ::/0 s0/1/0
```

Fuente: Autoría propia

Figura 26. Configuración inicial básica R3

The image shows a network configuration environment. On the left, a network diagram includes a router labeled 'Router3' (ISR4331) connected to a 'Troncal' switch (2950-S) via S0/1/1 and Fa0/3. A PC (PC-P) is connected to the switch. A table titled 'Definición de VLAN' is visible:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

The main part of the image is a 'Router3' CLI window titled 'IOS Command Line Interface'. The terminal output shows the following configuration steps:

```
Router>en  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#no ip domain-lookup  
Router(config)#en  
Router(config)#ena  
Router(config)#enable pass  
Router(config)#enable password class  
Router(config)#line con 0  
Router(config-line)#pass  
Router(config-line)#password cisco  
Router(config-line)#login  
Router(config-line)#exit  
Router(config)#serv  
Router(config)#service pas  
Router(config)#service password-encryption  
Router(config)#ban  
Router(config)#banner #Se prohíbe el acceso no autorizado#  
^  
% Invalid input detected at '^' marker.  
Router(config)#banner motd #Se prohíbe el acceso no autorizado#  
Router(config)#
```

The bottom of the image shows a Windows taskbar with the system clock at 8:30 p.m. on 23/11/2021.

Fuente: Autoría propia

Figura 27. Configuración R3 en proceso

The image shows a network configuration interface. On the left, a network diagram illustrates the topology: a server (Server-PT) is connected to Router2 (ISR4331) via G0/0. Router2 is connected to Router3 (ISR4331) via S0/1/1. Router3 is connected to a switch (2951-24) via S0/1/0. The switch is connected to a PC (PC-PT) via Fa0/18. A trunk link connects the switch to another switch (2951-24) via Fa0/3. A table titled 'Definición de VLAN' is visible in the background:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

The main window displays the CLI for Router3, showing the following configuration commands:

```
Router(config)#en
Router(config)#ena
Router(config)#enable pass
Router(config)#enable password class
Router(config)#line con 0
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#serv
Router(config)#service pas
Router(config)#service password-encryption
Router(config)#ban
Router(config)#banner #Se prohíbe el acceso no autorizado#

% Invalid input detected at '^' marker.

Router(config)#banner motd #Se prohíbe el acceso no autorizado#
Router(config)#
Router(config)#
Router(config)#hos
Router(config)#hostname R3
R3(config)#
R3(config)#line vty 0 4
R3(config-line)#pass
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#
```

Fuente: Autoría propia

Figura 28. Configuración finalizada de R3

The image shows a network configuration interface with two main windows. The top window, titled 'Definición de VLAN', contains a table with the following data:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

The bottom window, titled 'Router3', shows the CLI configuration for the router. The configuration includes:

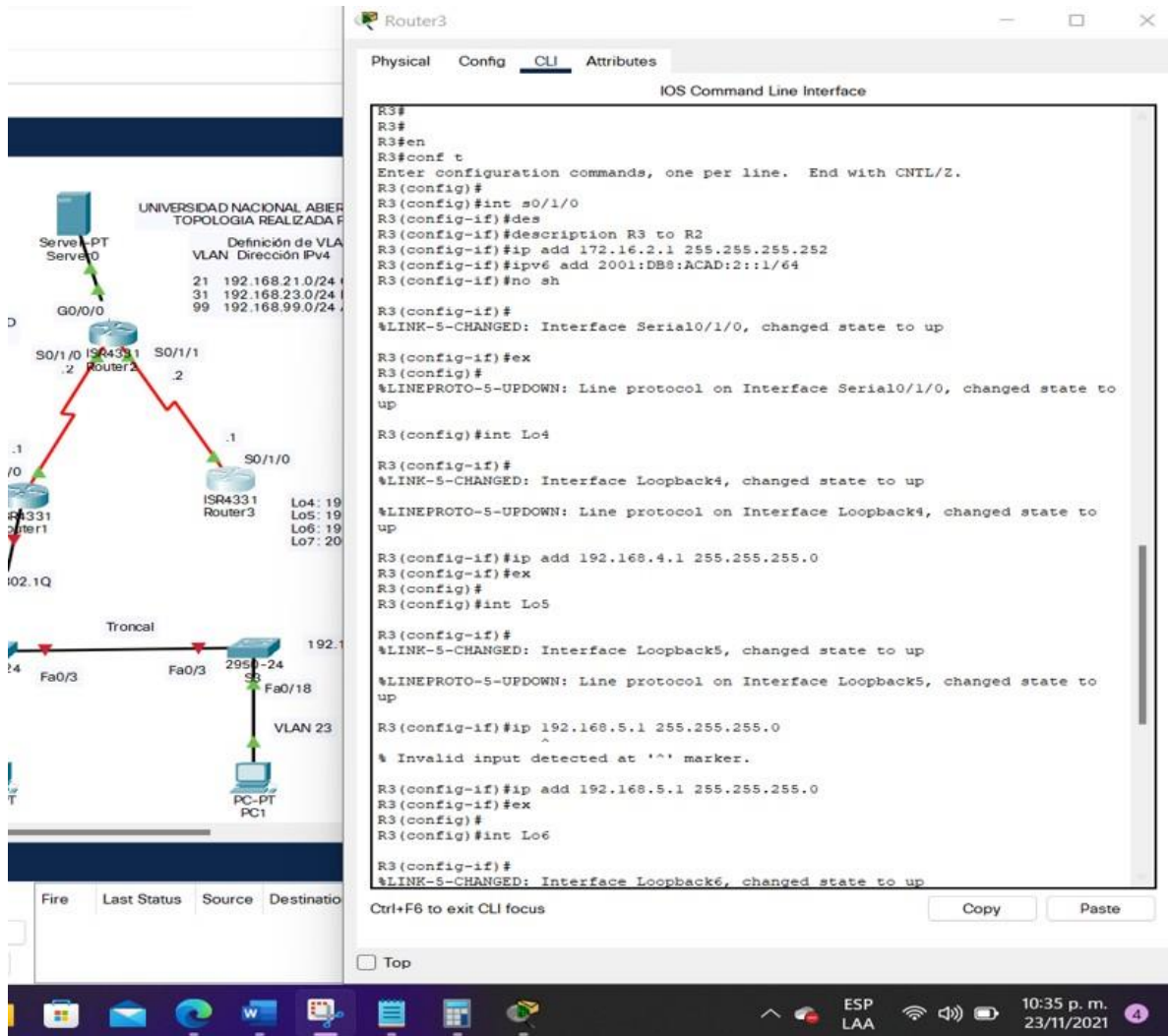
```
R3#wr
Building configuration...
[OK]
R3#
R3#sh ru
Building configuration...

Current configuration : 941 bytes
!
version 16.6.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable password 7 0622404F1A0A
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
```

The background shows a network diagram with Router3 (ISR4331) connected to a switch (2951-24) and a PC (PC-PT PC1). The switch is configured with VLAN 23. The router has interfaces S0/1/0, S0/1/1, Fa0/3, and Fa0/18. The PC is connected to Fa0/18.

Fuente: Autoría propia

Figura 29. Configuración de interfaz en R3



Fuente: Autoría propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

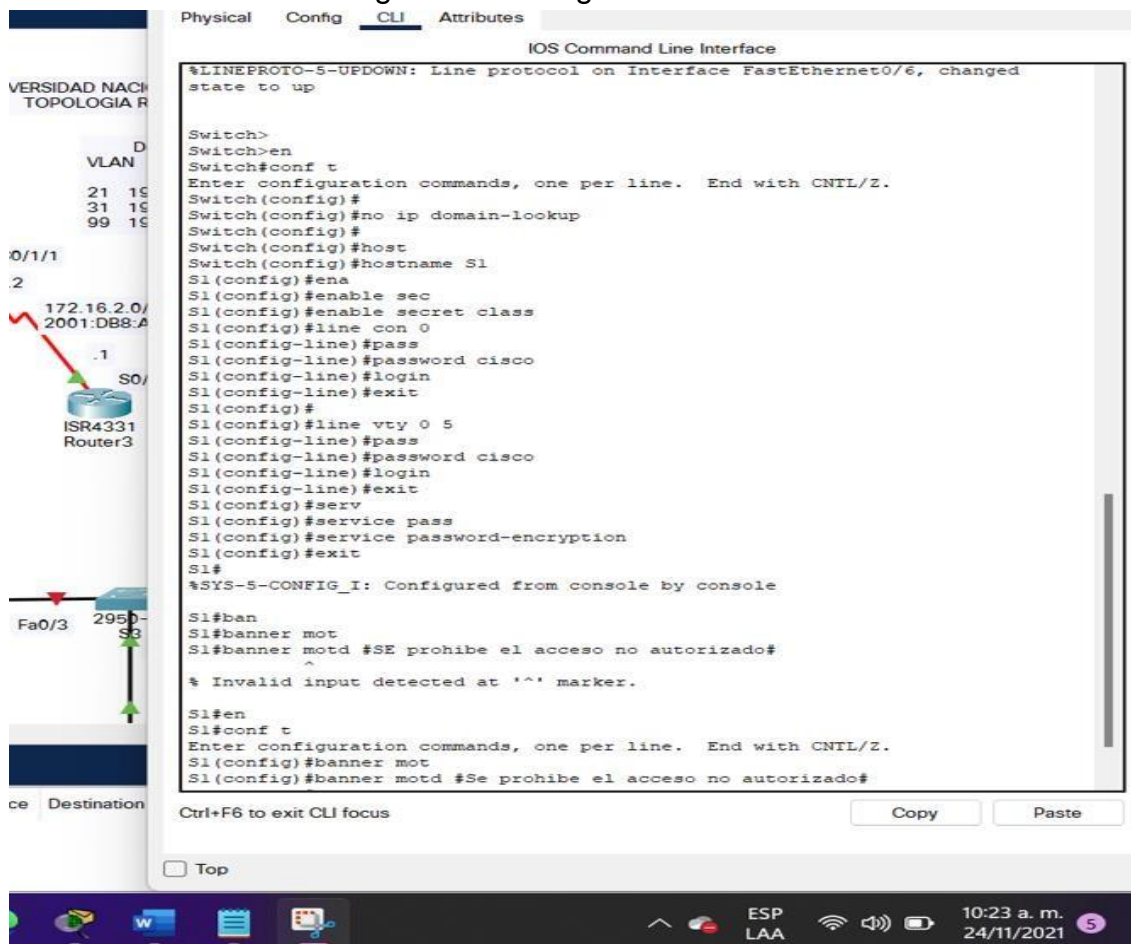
Tabla 10. Tareas de configuración S1

Elementos o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la	S1(config)#line con 0

consola	S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 5 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Autoría propia

Figura 30. Configuración básica S1



Fuente: Autoría propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 11. Tareas de configuración S3

Elementos o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 5 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Autoría propia

Figura 31. Configuración básica S3

```
IOS Command Line Interface

Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK061020WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up

Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
S3(config)#line vty 0 5
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
S3(config)#service password-encryption
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#en
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#do wr
Building configuration...
[OK]
S3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

W [Taskbar icons] ESP IAA [System tray] 10:30 a. m. 24/11/2021 [Clock]

Fuente: Autoría propia

Paso 7: Verificar la conectividad de la red.

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Tabla de Verificación de conectividad

Desde	A	Dirección IP	Resultados del ping
R1	R2, S0/1/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/18 ms
R2	R3, S0/1/0	172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/30 ms
Server de Internet	Gateway predeterminado	209.165.200.233	R3#ping 209.165.200.233 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 209.165.200.233, timeout is 2

			seconds: !!!! Success rate is 100 percent (5/5), round- trip min/avg/max = 1/3/12 ms
--	--	--	---

Fuente: Autoría propia

Figura 32. Uso del comando ping R1

Definición de VLAN

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

Router1 CLI Output:

```

Press RETURN to get started.

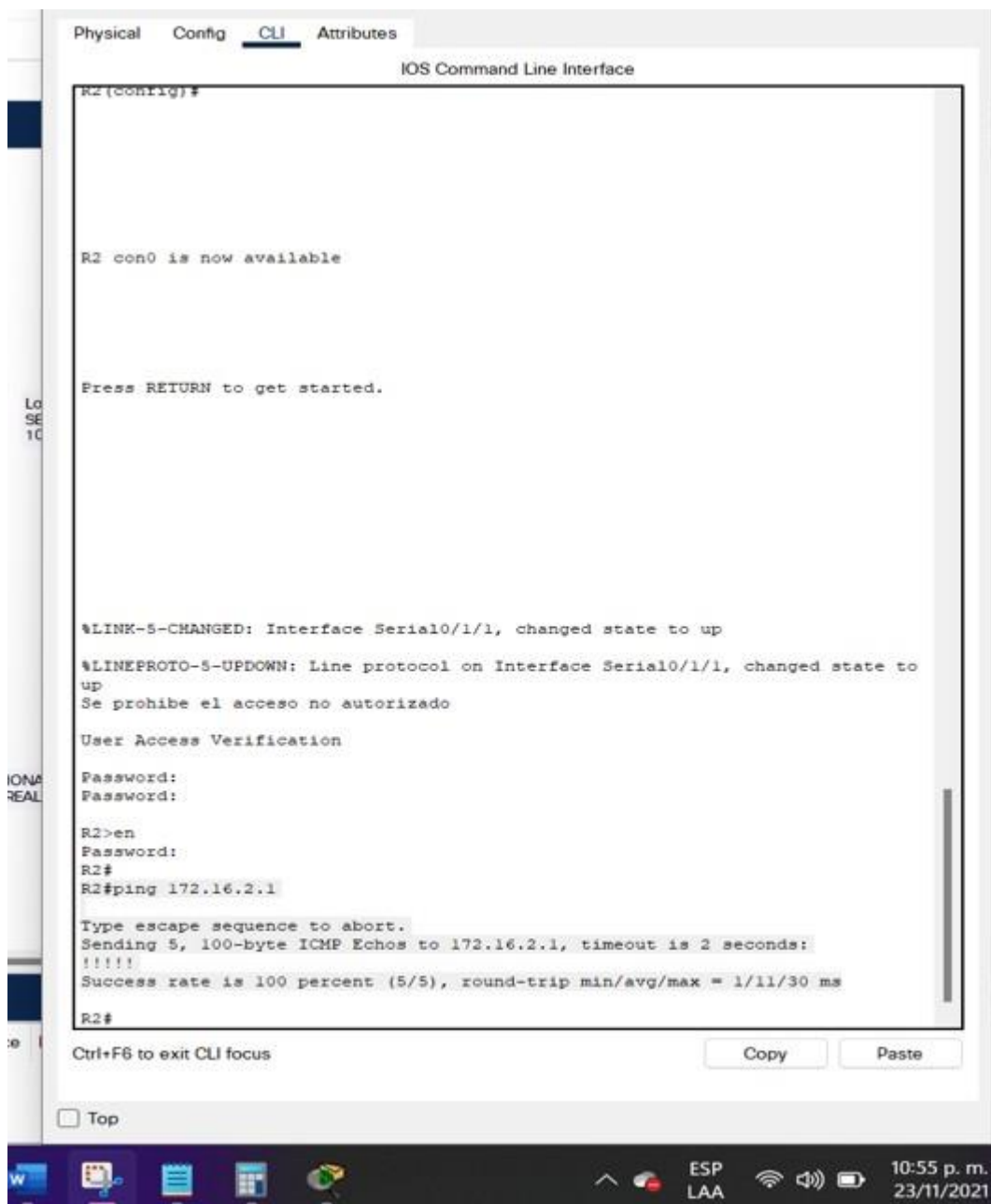
Se prohíbe el acceso no autorizado
User Access Verification
Password:
R1>ena
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/18 ms
R1#

```

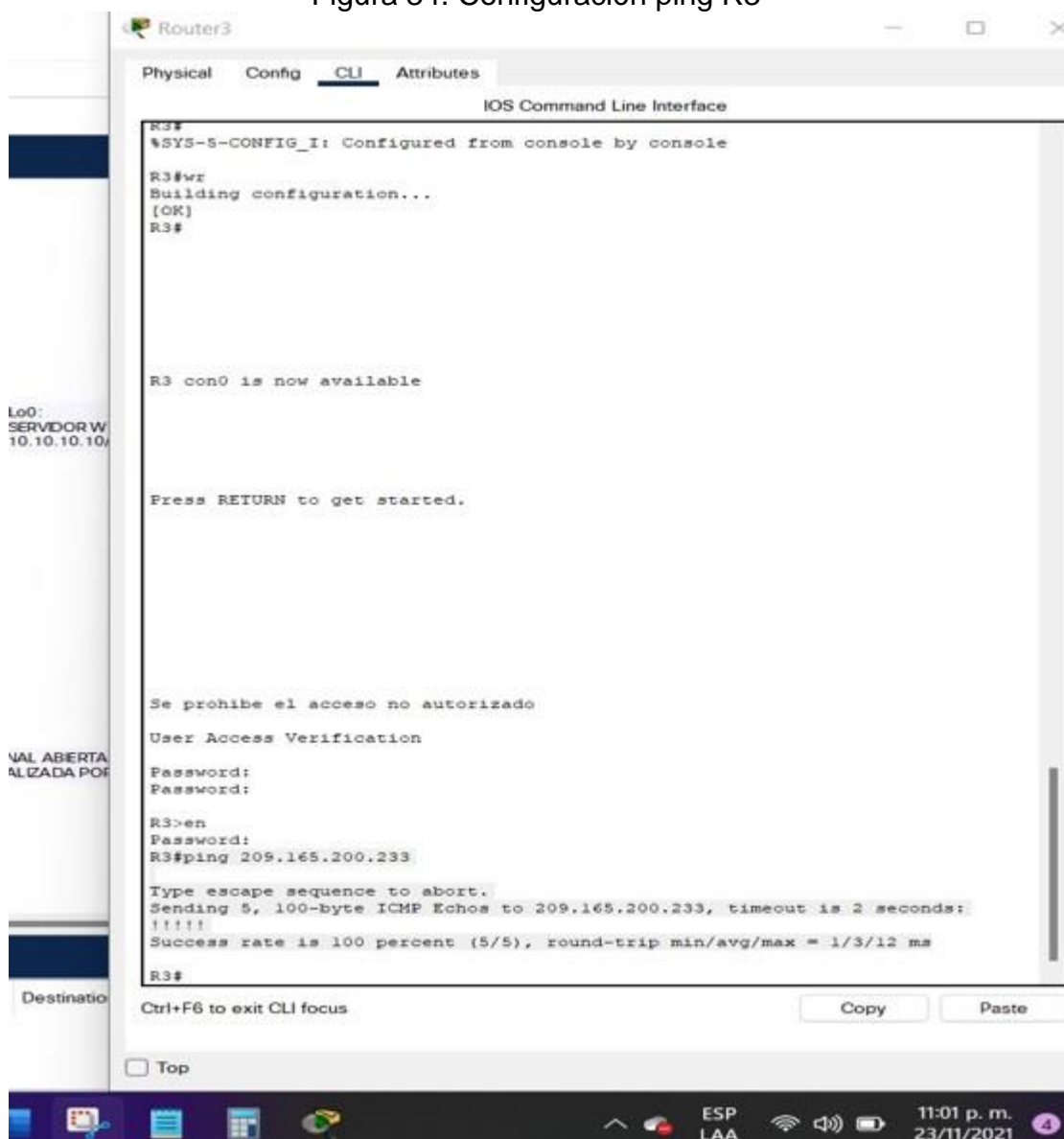
Fuente: Autoría propia

Figura 33. Configuración comando ping R2



Fuente: Autoría propia

Figura 34. Configuración ping R3



Fuente: Autoría propia

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Parte 3: Configurar la seguridad del switch, las VLAN y el routing.

entre VLAN Paso 1: Configurar S1. La configuración del S1 incluye

las siguientes tareas:

Tabla 13. Tareas de configuración S1, VLAN y routing

Elementos o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface F0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface F0/5 S1(config-if)#switch mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range F0/1-2, F0/4, F0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface F0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range F0/1-2, F0/4, F0/7-24 S1(config-if-range)#shutdown

Fuente: Autoría propia

Figura 35. Switch sin configuración Vlan

The image displays a network diagram on the left and a CLI screenshot on the right. The network diagram shows three routers (BR4331, Router2, Router3) connected via their S0/1/0 interfaces. Router2 is connected to Router1 and Router3. Router1 is connected to a switch (S2951-24) via its G0/1 interface. The switch has two VLANs: VLAN 21 (connected to PC0) and VLAN 2 (connected to PC1). The switch is connected to Router3 via its Fa0/3 interface. The CLI screenshot shows the configuration of the switch, including the default VLAN configuration and the status of various VLANs.

```
S1#  
Building configuration...  
[OK]  
S1#  
S1#  
S1#  
S1#  
S1#  
S1#conf t  
Enter configuration commands, one per line. End with CTRL/Z.  
S1(config)#  
S1(config)#  
S1(config)#EX  
D1#  
%SYS-5-CONFIG_I: Configured from console by console  
S1#  
S1#EN  
S1#SH VLAN
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	0	0
1004	fddnet	101004	1500	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	lsm	-	0	0

```
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2  
-----  
Remote SPAN VLANs  
-----  
PRIMARY Secondary Type Ports  
S1#
```

Fuente: Autoría propia

Figura 36. Switch configuración de Vlan

The image shows a network configuration environment. On the left, a network diagram illustrates a topology with three routers (ISR4331, Router2, Router3) and a switch (S3). A table titled 'Definición de VLAN' lists the following:

VLAN	Dirección IPv4	Nombre
21	192.168.21.0/24	Contabilidad
31	192.168.23.0/24	Ingeniería
99	192.168.99.0/24	Administración

On the right, the CLI window for switch S1 shows the following configuration commands:

```

S1(config)#int range f0/1-2, f0/4, f0/6-24
S1(config-if-range)#sw
S1(config-if-range)#switchport mod
S1(config-if-range)#switchport mode acc
S1(config-if-range)#switchport mode access
S1(config-if-range)#ex
S1(config)#
S1(config)#sw
S1(config)#sw
S1(config)#int f0/6
S1(config-if)#sw
S1(config-if)#switchport acc
S1(config-if)#switchport access vlan 21
S1(config-if)#ex
S1(config)#
S1(config)#int f0/1-2, f0/4, f0/7-24
S1(config)#
% Invalid input detected at '^' marker.
S1(config)#int ra f0/1-2, f0/4, f0/7-24
S1(config-if-range)#sh
S1(config-if-range)#
S1(config-if-range)#ex
S1(config)#ex
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#sh vlan
-----
VLAN Name                Status      Ports
-----
1    default                 active      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23, Fa0/24
21   Contabilidad            active      Fa0/6
23   Ingenieria              active
99   Administrativa          active
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default        active
    
```

Fuente: Autoría propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14. Tareas de configuración S3

Elementos o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre> S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit </pre>

Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2,fa0/4- 24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1- 2,fa0/4- 17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Fuente: Autoría propia

Figura 37. Configuración S3

```
IOS Command Line Interface
Power supply serial number: LRB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHR061020RC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharizba

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up

Switch>
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
S3(config)#line vty 0 5
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
S3(config)#service password-encryption
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#en
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#do wr
Building configuration...
[OK]
S3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Autoría propia

Figura 38. Configuración completa S3

The network diagram shows three routers (ISR4331) and a switch (S3). Router 1 is connected to Router 2 and Router 3. Router 2 is connected to Router 3. Router 3 is connected to switch S3. Switch S3 is connected to a PC (PC-PT) via VLAN 23. The CLI window shows the configuration for S3, including interface ranges, access VLANs, and status messages for various interfaces.

```

S3
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

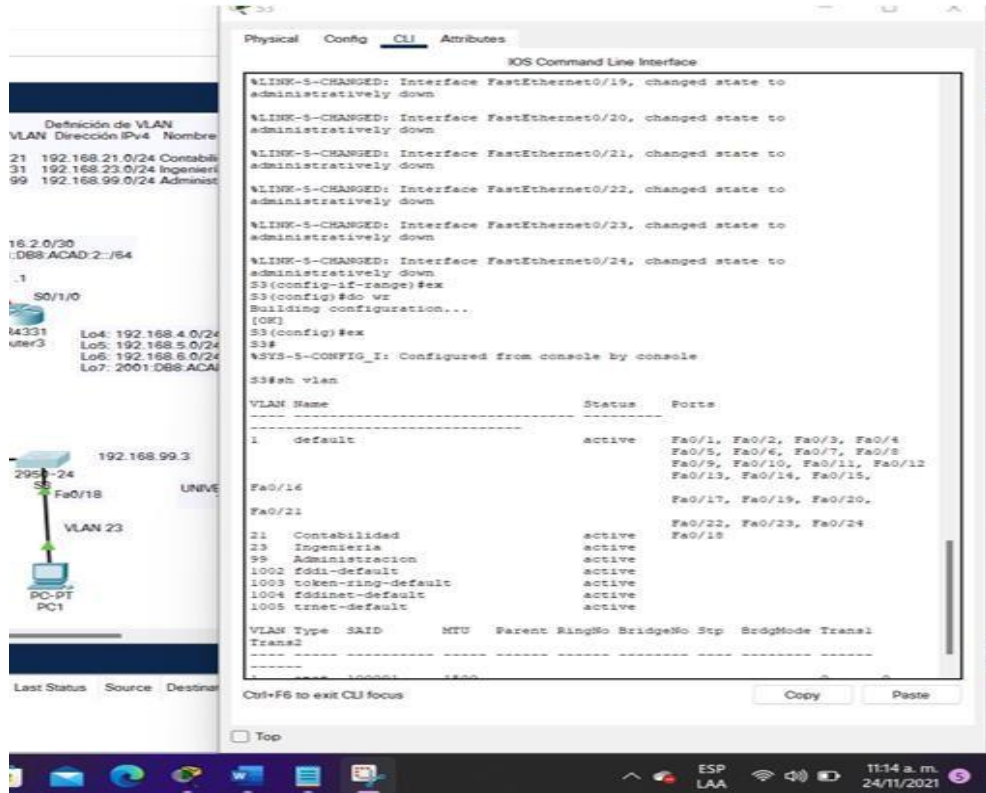
S3(config-if)#ex
S3(config)#
S3(config)#int fa
S3(config-if-range)#sw mode ac
S3(config-if-range)#sw mode access
S3(config-if-range)#int f0/18
S3(config-if)#sw a
S3(config-if)#sw access vlan 21
S3(config-if)#ex
S3(config)#int fa
S3(config)#int range f0/1-2, f0/4-17, f0/19-24
S3(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively
down

Ctrl+F6 to exit CLI focus
Copy Paste
    
```

Fuente: Autoría propia

Figura 39. Configuración base de datos Vlan



Fuente: Autoría propia

Paso 3: Configurar R1 Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Tabla de configuración de R1

Elementos o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Descripción: LAN de Contabilidad Asignar la VLAN 21</p> <p>Asignar la primera dirección disponible a esta interfaz</p> <pre> R1(config)#int G0/0/1.21 R1(config-subif)#description accounting LAN R1(config-subif)#enc R1(config-subif)#encapsulation R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit </pre>

<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p>	<p>Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)# R1(config)#int G0/0/1.23 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#exit R1(config)#</p>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<p>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config)#int G0/0/1.99 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit</p>
<p>Activar la interfaz G0/1</p>	<p>R1(config)# R1(config)#int G0/0/1</p>

```
R1(config-if)#no sh
R1(config-if)#exit
R1#wr
Building configuration...
[OK]
R1#
```

Fuente: Autoría propia

Figura 40. Configuración R1



Fuente: Autoría propia

Figura 41. Configuración interfaz R1

The image displays a network configuration interface for Router1. The main window shows the CLI with the following configuration:

```
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0/1.21
description accounting LAN
encapsulation dot1Q 21
ip address 192.168.21.1 255.255.255.0
!
interface GigabitEthernet0/0/1.23
description accounting LAN
encapsulation dot1Q 23
ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet0/0/1.99
description accounting LAN
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
--More--
```

The background shows a network topology diagram with two routers, Router1 and Router2, connected via a serial link. Router1 is connected to a switch (SW1) and a trunk link (Troncal) with Fa0/3. The switch is connected to a PC (PC1) and a server (Server1). The diagram also shows VLAN information: VLAN 21, 31, and 99. The IP address 172.16.2.2001 is associated with the switch.

Fuente: Autoría propia

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 16. Tabla Verificación de conectividad de red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:

			!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Fuente: Guía de actividades

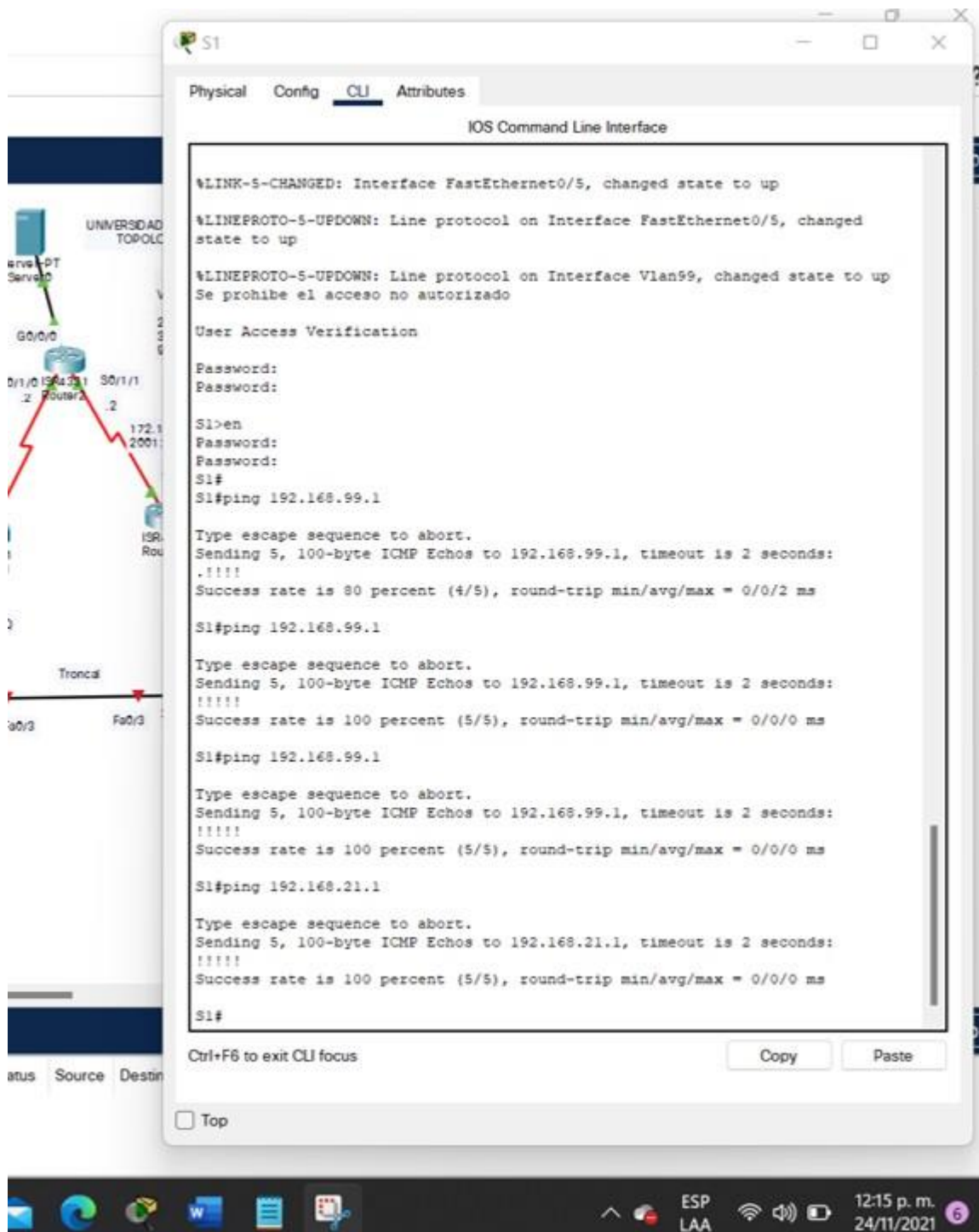
Figura 42. Configuración de conectividad R1

The image shows a network configuration interface. On the left, a topology diagram titled 'UNIVERSIDAD NA TOPOLOGIA' shows a central router 'R1' connected to three other routers: 'R2', 'R3', and 'R99'. R1 is connected to R2 via S0/1/0 and R2 to R1 via S0/1/1. R1 is connected to R3 via S0/1/0 and R3 to R1 via S0/1/1. R1 is connected to R99 via S0/1/0 and R99 to R1 via S0/1/1. A 'Troncal' link is shown between R1 and R99. On the right, a CLI window for 'Router1' shows the configuration of interfaces GigabitEthernet0/0/1, 21, 23, and 99, and Serial0/1/0. The configuration includes descriptions, encapsulation, and IP addresses. Below the configuration, the CLI shows the execution of ping commands to 192.168.99.1, 192.168.23.1, and 192.168.21.1, all resulting in 100% success rates. The CLI window also shows a 'Copy' and 'Paste' button and a 'Ctrl+F6 to exit CLI focus' message.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0/1.21
description accounting LAN
encapsulation dot1Q 21
ip address 192.168.21.1 255.255.255.0
!
interface GigabitEthernet0/0/1.23
description accounting LAN
encapsulation dot1Q 23
ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet0/0/1.99
description accounting LAN
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
R1#
R1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/14 ms
R1#ping 192.168.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/8/15 ms
R1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/14 ms
R1#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

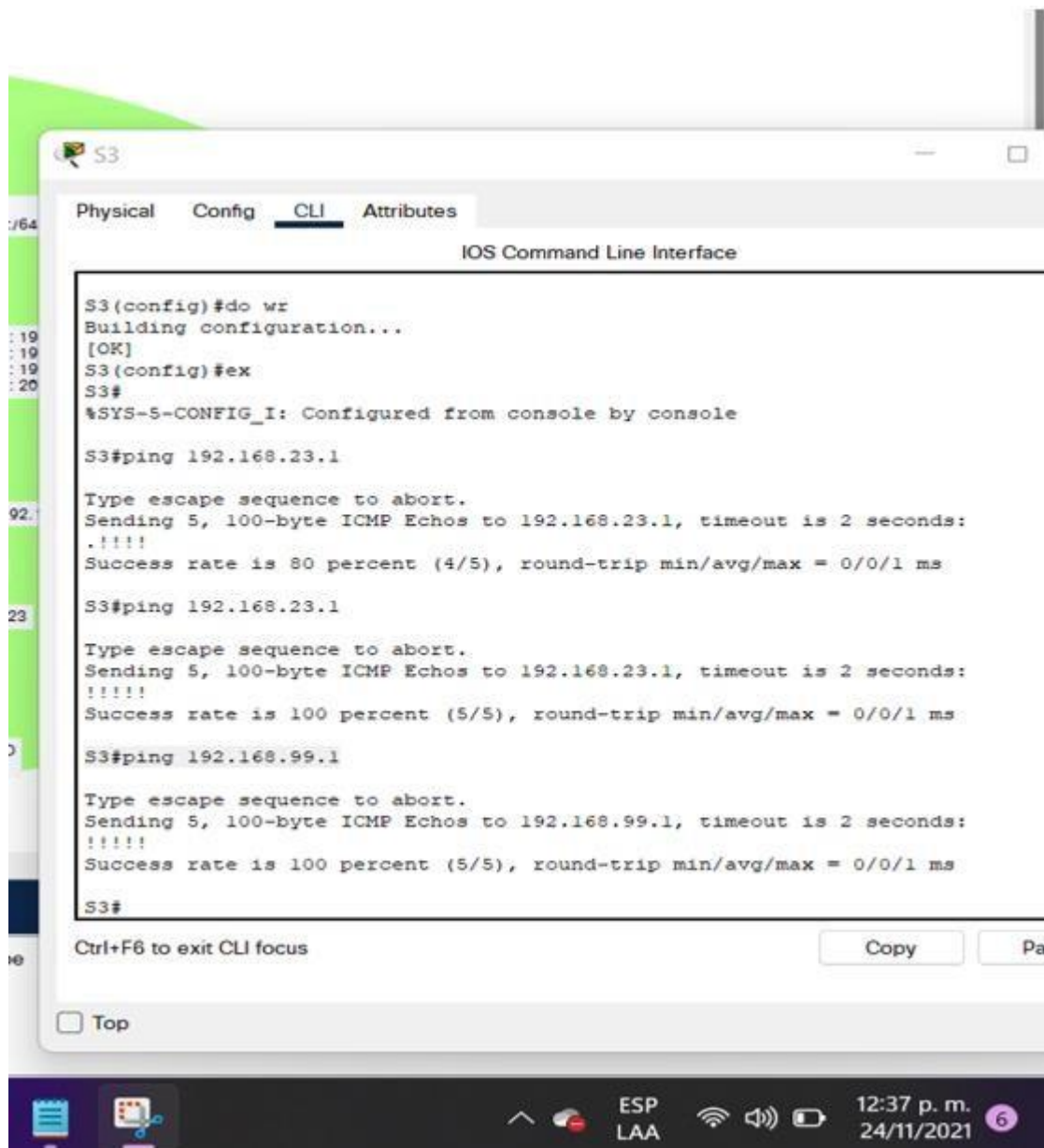
Fuente: Autoría propia

Figura 43. Configuración de conectividad S1



Fuente: Autoría propia

Figura 44. Configuración de conectividad S3



The screenshot shows a terminal window titled 'S3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user enters the command 'do wr', which saves the configuration. Then, they enter 'ex' to exit configuration mode. A system message indicates the configuration was saved from the console. The user then performs three ping tests: first to 192.168.23.1 (80% success rate), then to 192.168.23.1 again (100% success rate), and finally to 192.168.99.1 (100% success rate). The terminal output shows the details of each ping, including the number of packets sent and the success rate. At the bottom of the window, there are buttons for 'Copy' and 'Pa' (Paste), and a 'Top' button. The system tray at the bottom of the screen shows the time as 12:37 p.m. on 24/11/2021 and a notification icon with the number 6.

```
S3
Physical Config CLI Attributes
IOS Command Line Interface

S3(config)#do wr
Building configuration...
[OK]
S3(config)#ex
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.99.1

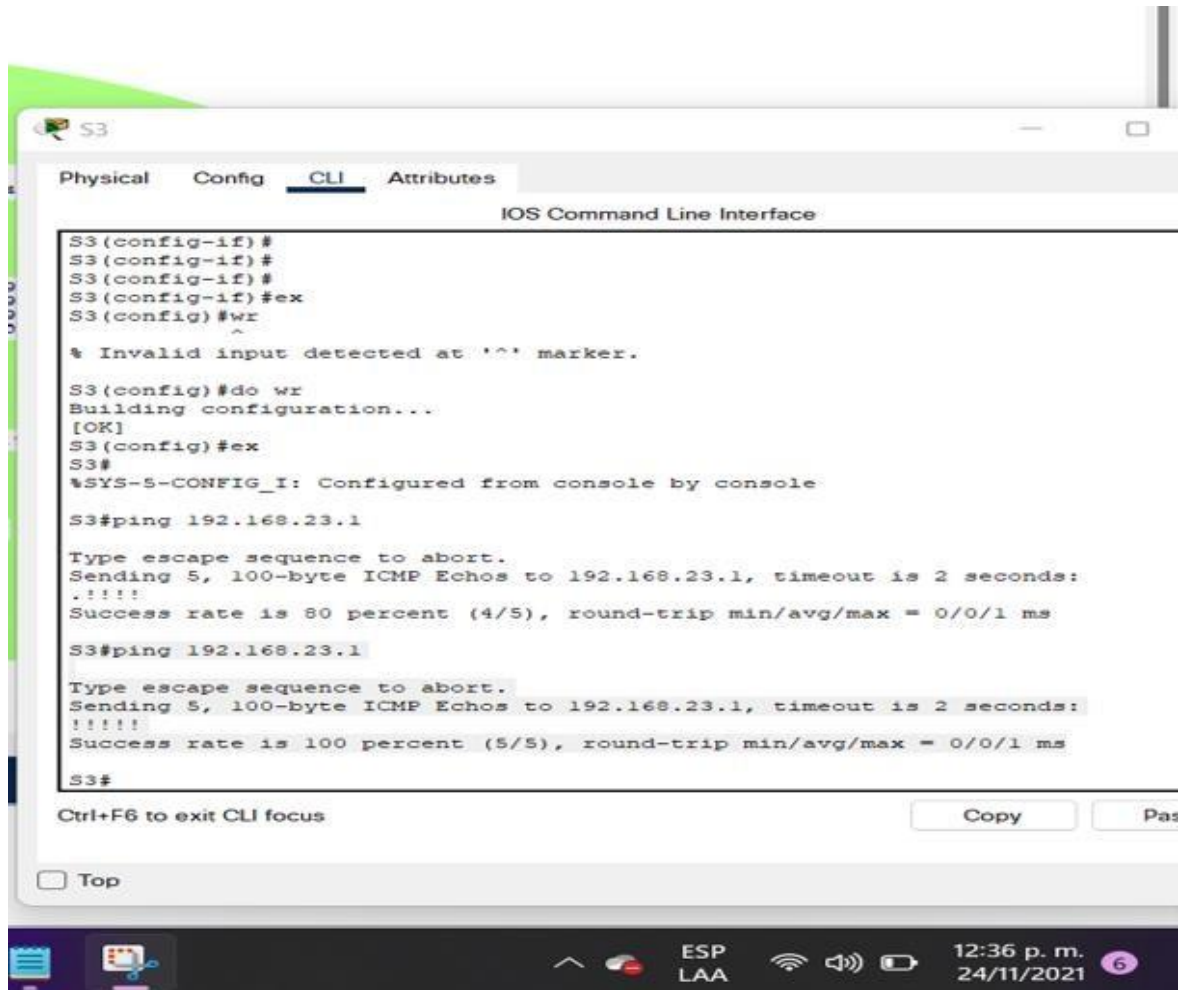
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#

Ctrl+F6 to exit CLI focus
Copy Pa
Top
```

Fuente: Autoría propia

Figura 45. Configuración de conectividad S3 finalizada



Fuente: Autoría propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1 Las tareas de configuración

para R1 incluyen las siguientes:

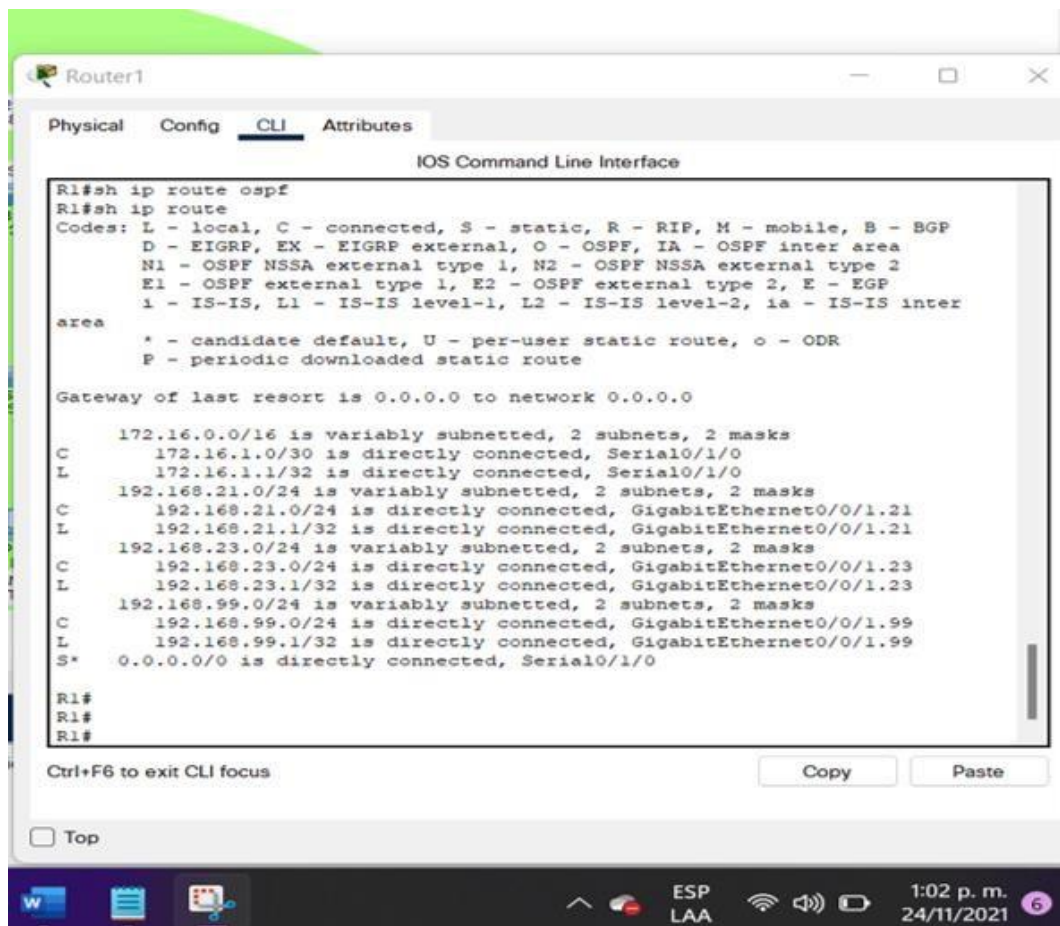
Tabla 17. Configuración de protocolo OSPF en R1

Elementos o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas	R1(config)#router OSPF 1 R1(config-router)#net 172.16.1.0 0.0.0.3 area 0 R1(config-router)#net 192.168.21.0 0.0.0.255

directamente	<pre> area 0 R1(config-router)#net 192.168.23.0 0.0.0.255 area 0 R1(config-router)#net 192.168.99.0 0.0.0.255 area 0 R1(config-router)# </pre>
Establecer todas las interfaces LAN como pasivas	<pre> R1(config-router)#passive-interface G0/0/1.21 R1(config-router)#passive-interface G0/0/1.23 R1(config-router)#passive-interface G0/0/1.99 R1(config-router)# </pre>
Desactive la Sumarización automática	A diferencia de EIGRP y RIPv1 y RIPv2. OSPF no admite el resumen automático. Por tanto, no es posible deshabilitar el auto resumen o Sumarización.

Fuente: Autoría propia

Figura 46. Configuración de OSPF en R1



Fuente: Autoría propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

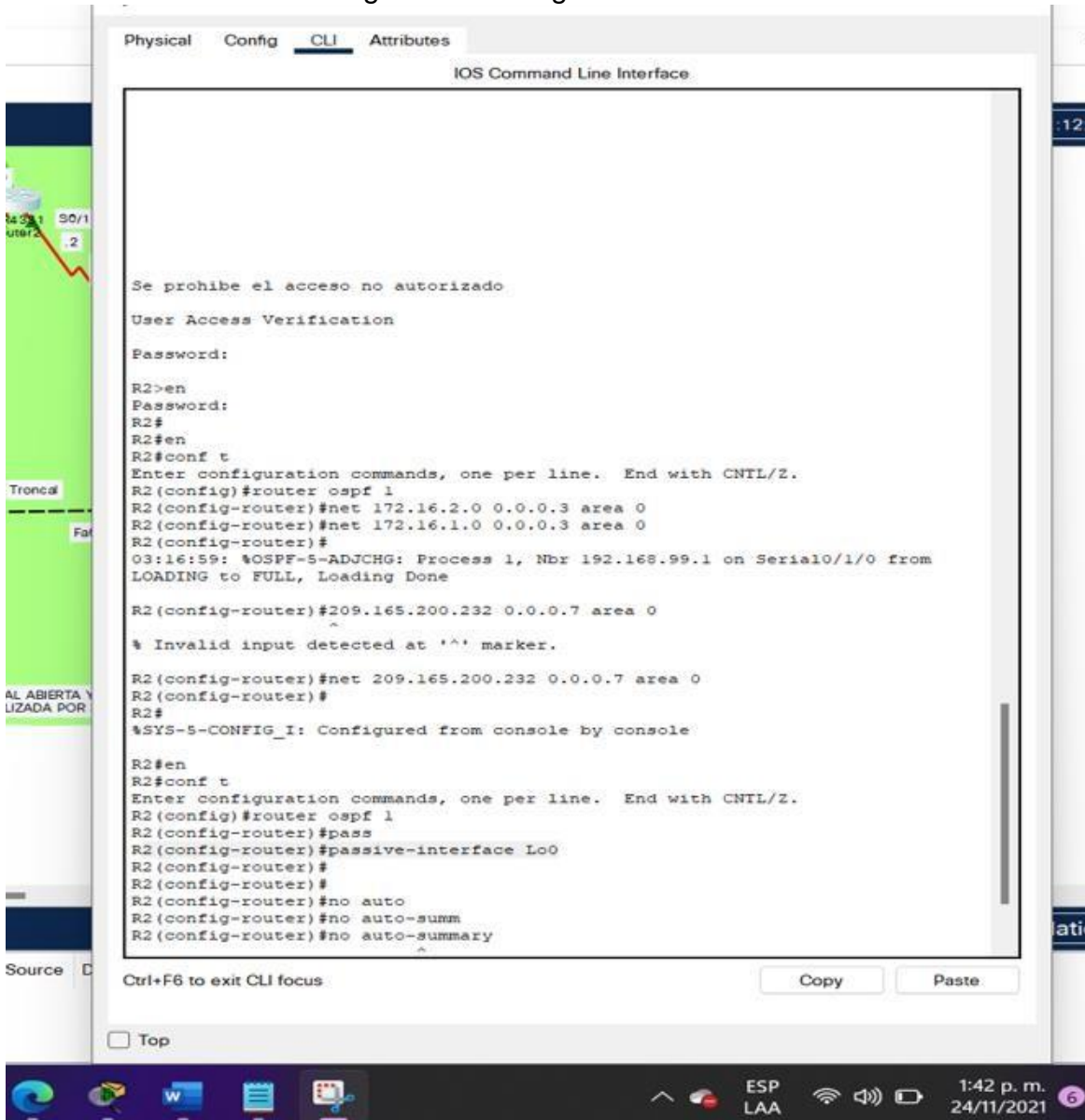
Tabla 18. Configuración de protocolo OSPF en R2

Elementos o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#net 172.16.2.0 0.0.0.3 area 0 R2(config-router)#net 172.16.1.0 0.0.0.3 area 0 R2(config-router)# 03:16:59: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/1/0 from LOADING to FULL, Loading Done R2(config-router)#net 209.165.200.232 0.0.0.7 area 0 from console by console
Establecer todas las interfaces LAN (loopback) como pasivas	R2(config-router)#passive-interface Lo0
Desactive la Sumarización automática	A diferencia de EIGRP y RIP1Y RPIv2. OSPF no admite el resumen automático. Por tanto, no es posible deshabilitar el auto resumen o Sumarización.

Fuente: Autoría propia

A diferencia de EIGRP y RIP1Y RPIv2. OSPF no admite el resumen automático. Por tanto, no es posible deshabilitar el auto resumen o Sumarización.

Figura 47. Configuración OSPF en R2



Fuente: Autoría propia

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 19. Tabla de configuración de OSPF en R2

Elementos o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4	R3(config-router)#net 172.16.2.0 0.0.0.3 area 0

conectadas directamente	R3(config-router)# 03:27:53: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/1/0 from LOADING to FULL, Loading Done net 192.168.4.0 0.0.0.255 area 0 R3(config-router)#net 192.168.6.0 0.0.0.255 area 0 R3(config-router)#
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface Lo4 R3(config-router)#passive-interface Lo5 R3(config-router)#passive-interface Lo6 R3(config-router)#
Desactive la Sumarización automática.	A diferencia de EIGRP y RIP1Y RPIv2. OSPF no admite el resumen automático. Por tanto, no es posible deshabilitar el auto resumen o Sumarización.

Fuente: Autoría propia

Paso 4: Verificar la información de OSPF

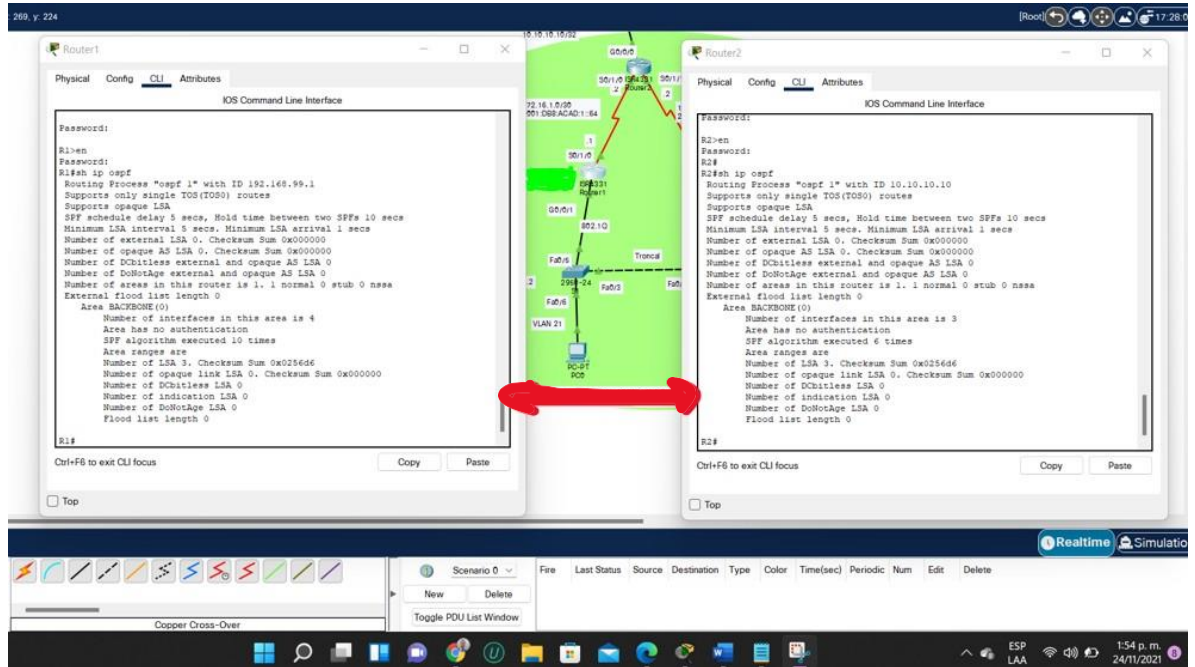
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 20. Tabla de verificación de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip opsf
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf database

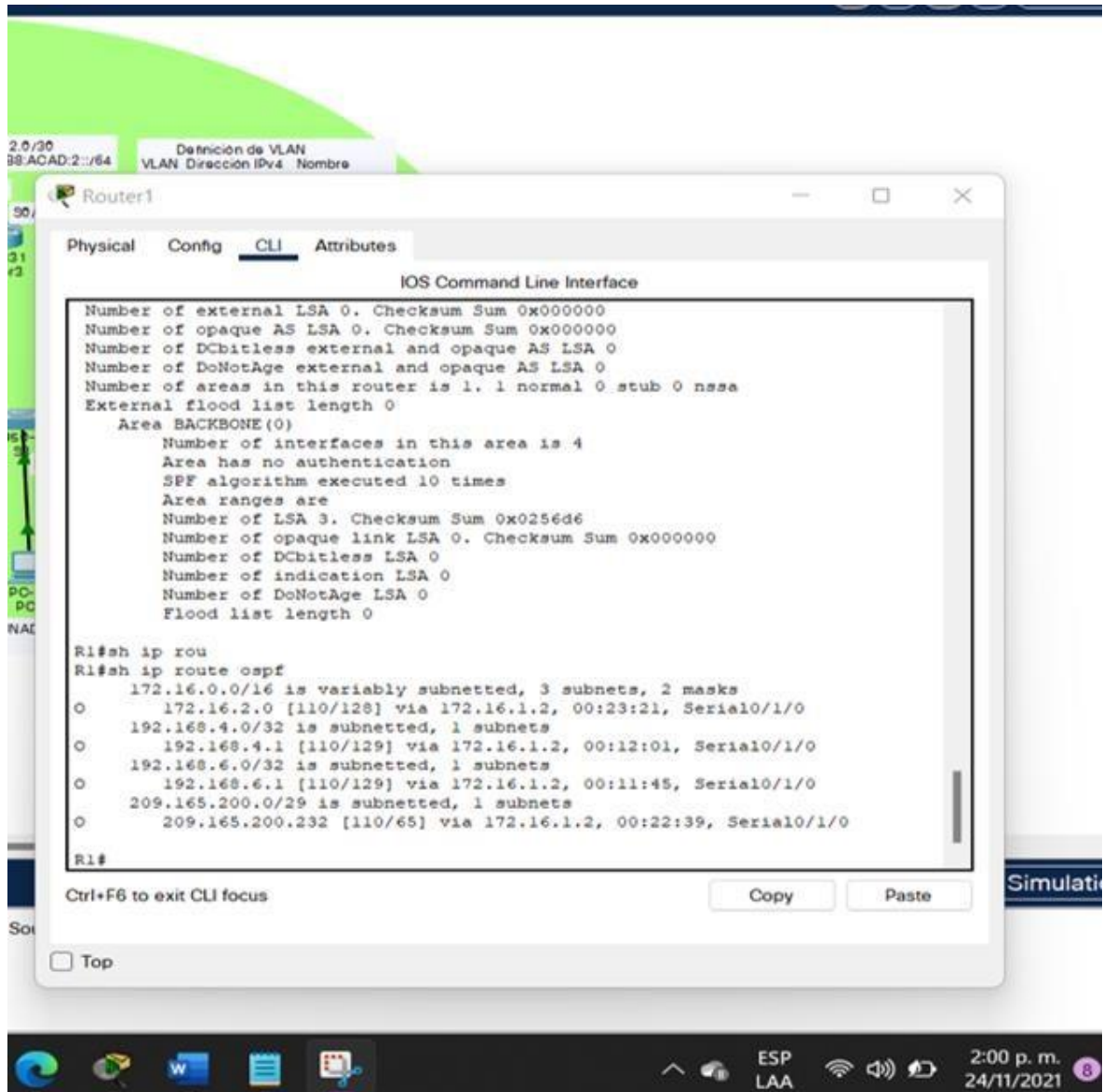
Fuente: Autoría propia

Figura 48. Configuración comando Show ip ospf



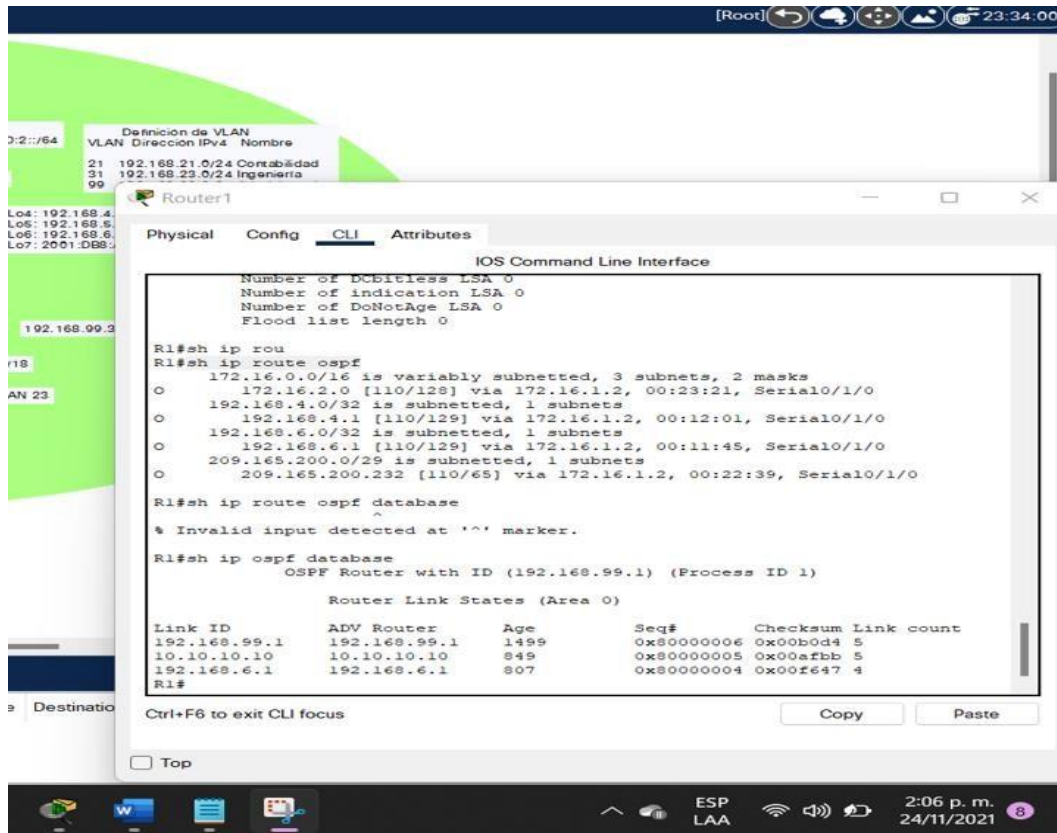
Fuente: Autoría propia

Figura 49. Configuración comando s hip route ospf



Fuente: Autoría propia

Figura 50. Comando show ospf database



Fuente: Autoría propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Tabla de R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30

para configuraciones estáticas	R1(config)#
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30 R1(config)#
Crear un pool de DHCP para la VLAN 21.	R1(config)# R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#def R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#net 192.168.21.0 255.255.255.0 R1(dhcp-config)#ex R1(config)#
Crear un pool de DHC.P para la VLAN 23	R1(config)# R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-ser R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domai R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#def R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#net 192.168.23.0 255.255.255.0 R1(dhcp-config)#ex

Fuente: Autoría propia

Figura 51. Configuración de R1 como DHCP

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R1>en
Password:
R1#
R1#en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#ip dhcp exc-add 192.168.21.1 192.168.21.30
      ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp exc
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
R1(config)#
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
R1(config)#
R1(config)#
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#def
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#net 192.168.21.0 255.255.255.0
R1(dhcp-config)#ex
R1(config)#
R1(config)#
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-ser
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domai
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#def
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#net 192.168.23.0 255.255.255.0
R1(dhcp-config)#ex
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#ex
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
[OK]
R1#
```

Fuente: Autoría propia

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 22. Tabla tareas de NAT estática y dinámica R2

Elementos o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco 12345
Habilitar el servicio del servidor HTTP	No, Soporta.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No, Soporta.
Crear una NAT estática al servidor web.	R2(config)# R2(config)#ip nat inside sou R2(config)#ip nat inside source st R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int G0/0/0 R2(config-if)#ip nat inside R2(config-if)#ex
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#acces R2(config)#access-list 1 per R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Definir la traducción de NAT dinámica	R2(config)# R2(config)#ip nat inside sou R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#
---------------------------------------	---

Fuente: Autoría propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

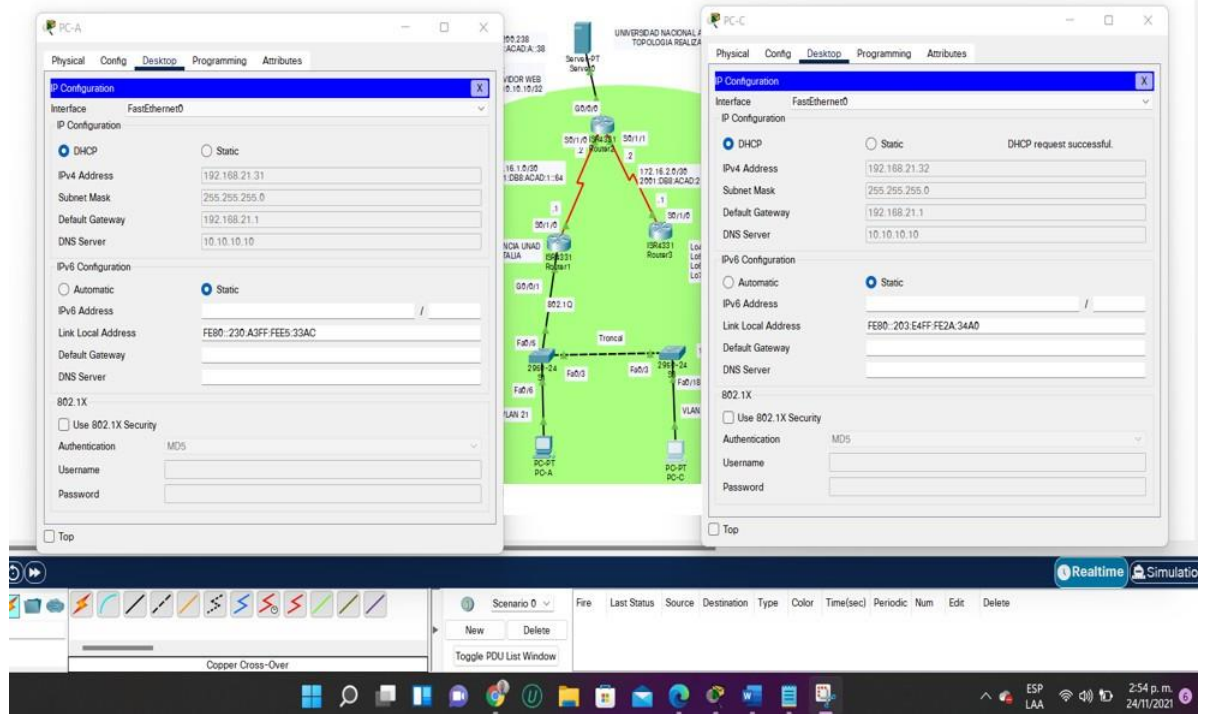
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 23. Verificación de DHCP y NAT

Elementos o tarea de configuración	Especificación
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	ok
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Ping 192.168.21.32
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

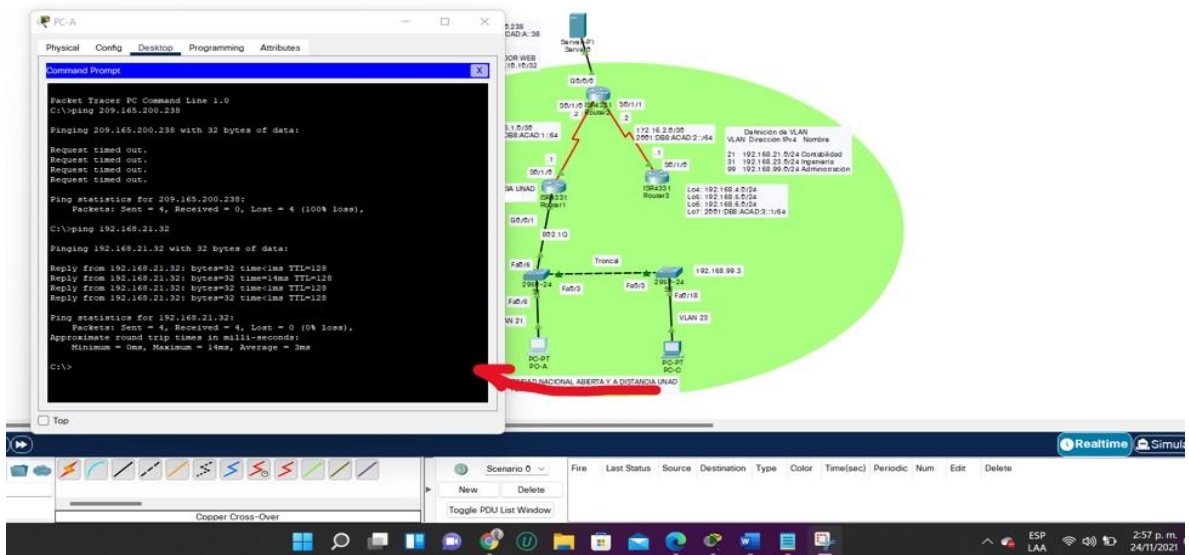
Fuente: Guía de actividades

Figura 52. Verificación de DHCP



Fuente: Autoría propia

Figura 53. Configuración comando Ping a IP 192.168.21.32



Fuente: Autoría propia

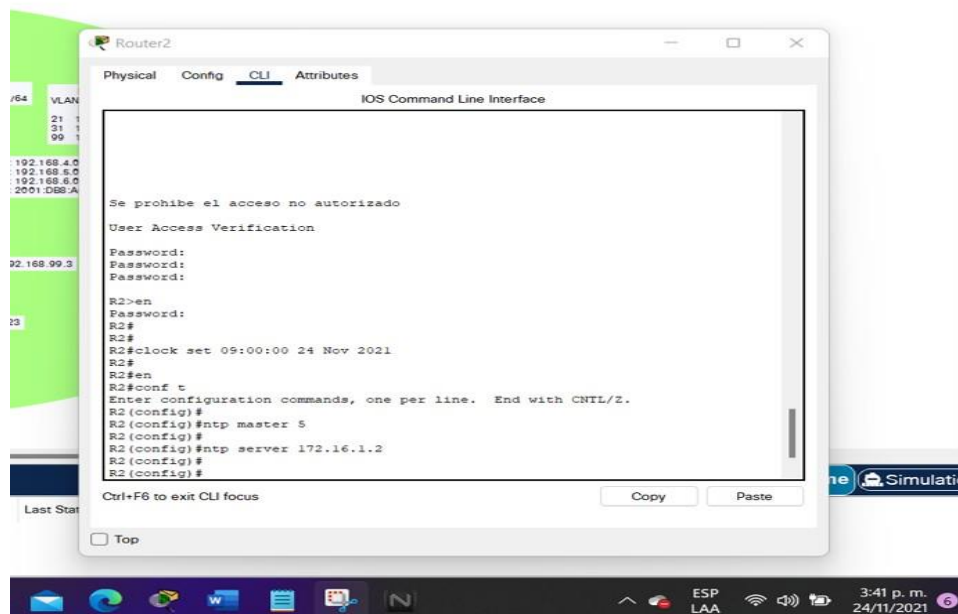
Parte 6: Configurar NTP

Tabla 24. Tabla de Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 24 Nov 2021
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R2(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#sh ntp status

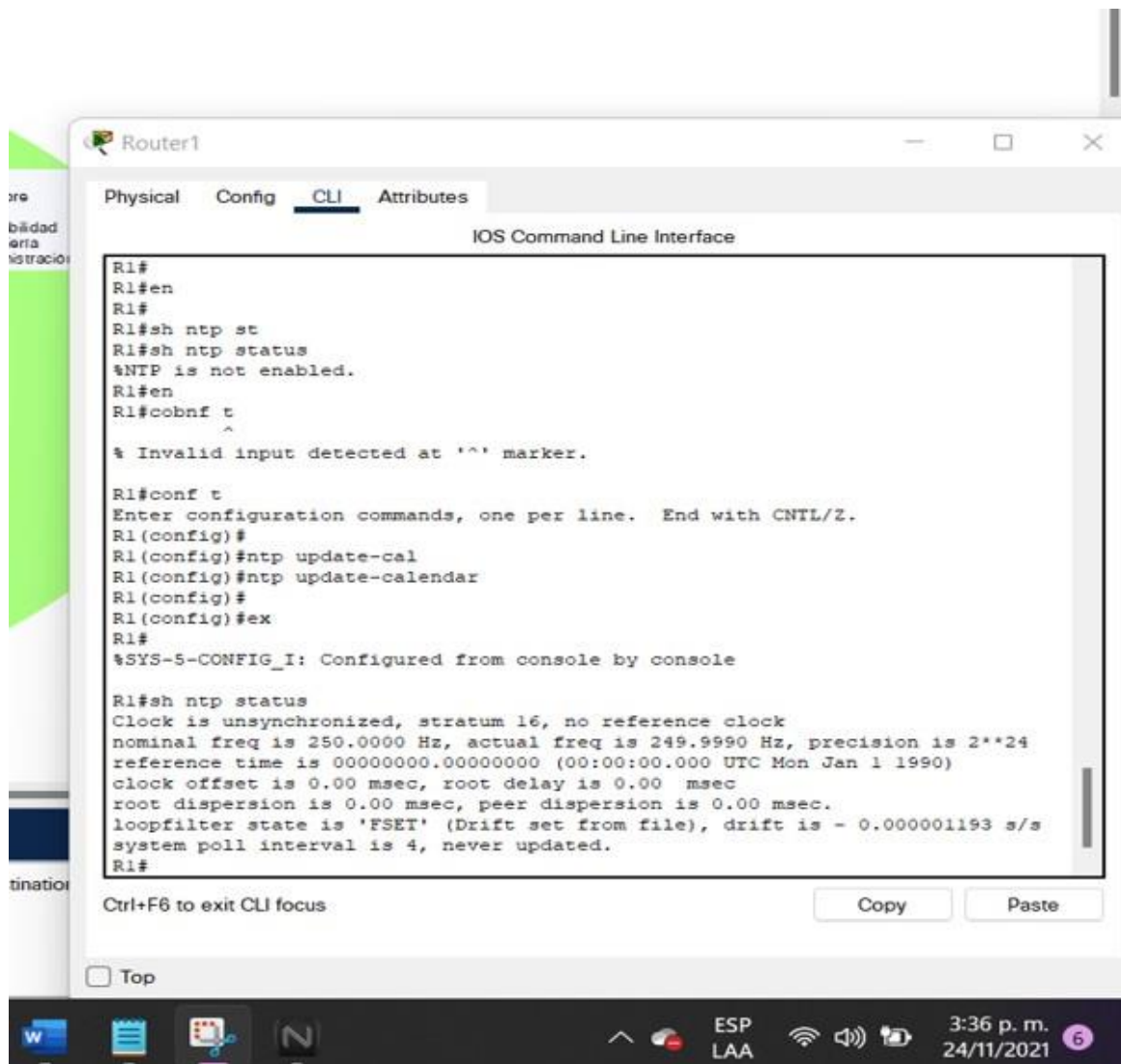
Fuente: Autoría propia

Figura 54. Configuración NTP



Fuente: Autoría propia

Figura 55. Configuración de NTP en R1



Fuente: Autoría propia

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

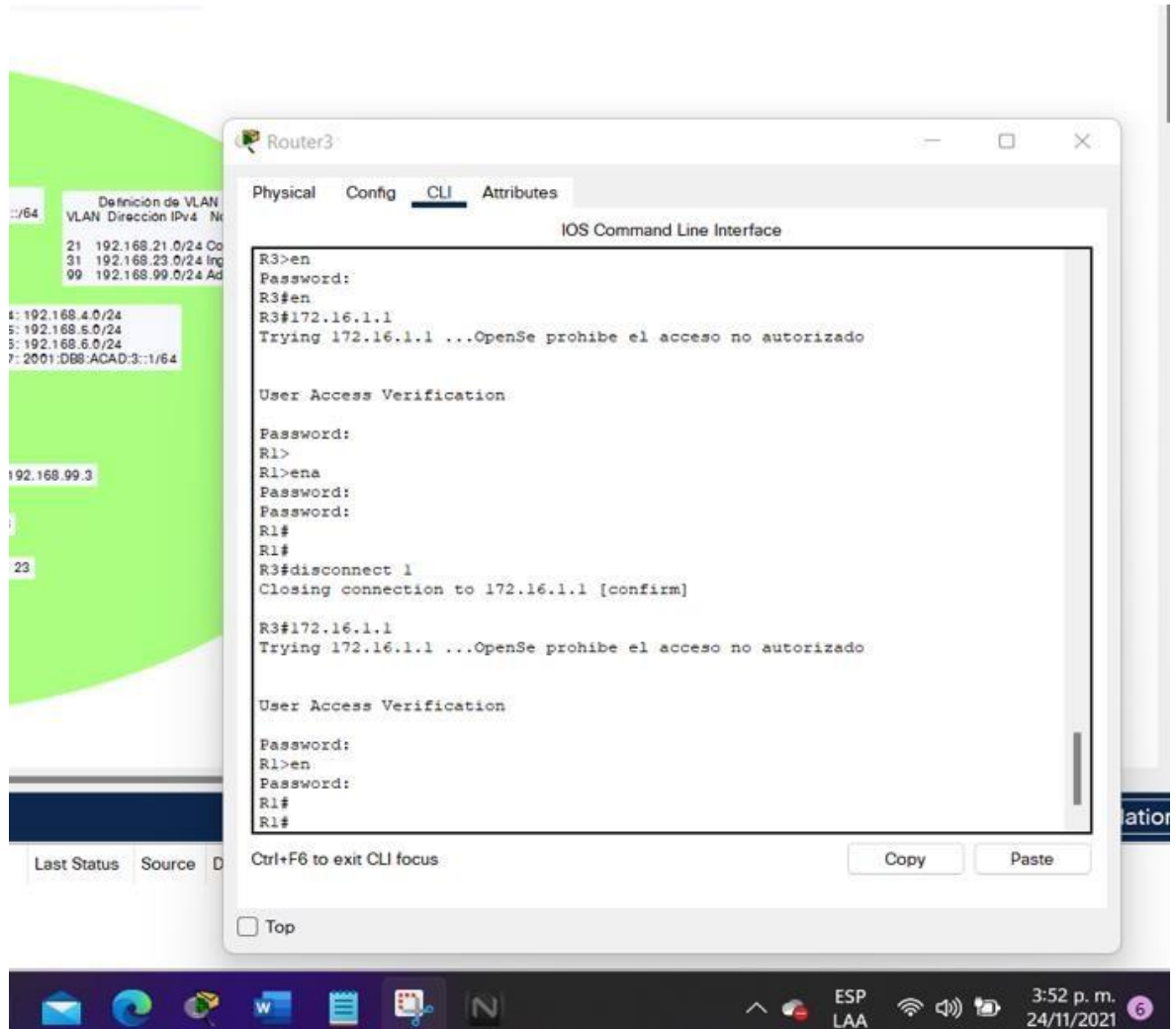
Paso 1: Restringir el acceso a las líneas VTY en R2.

Tabla 25. Tabla de configuración de listas de acceso

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN- MGT R2(config)# R2(config)#ip acc R2(config)#ip access-list stan R2(config)#ip access-list standard ADMIN- MGT R2(config-std-nacl)# R2# %SYS-5-CONFIG_I: Configured from console by console
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)# R2(config-std-nacl)#PERMIT HOST 172.16.1.1 R2(config-std-nacl)#EX
Permitir acceso por Telnet a las líneas de VTY	R2(config)#LINE VTY 0 4 R2(config-line)#ACC R2(config-line)#ACCES R2(config-line)#ACCESs-class ADMIN-MGT in R2(config-line)#ex % Ambiguous command: "ex" R2(config-line)#exit
Verificar que la ACL funcione como se espera	

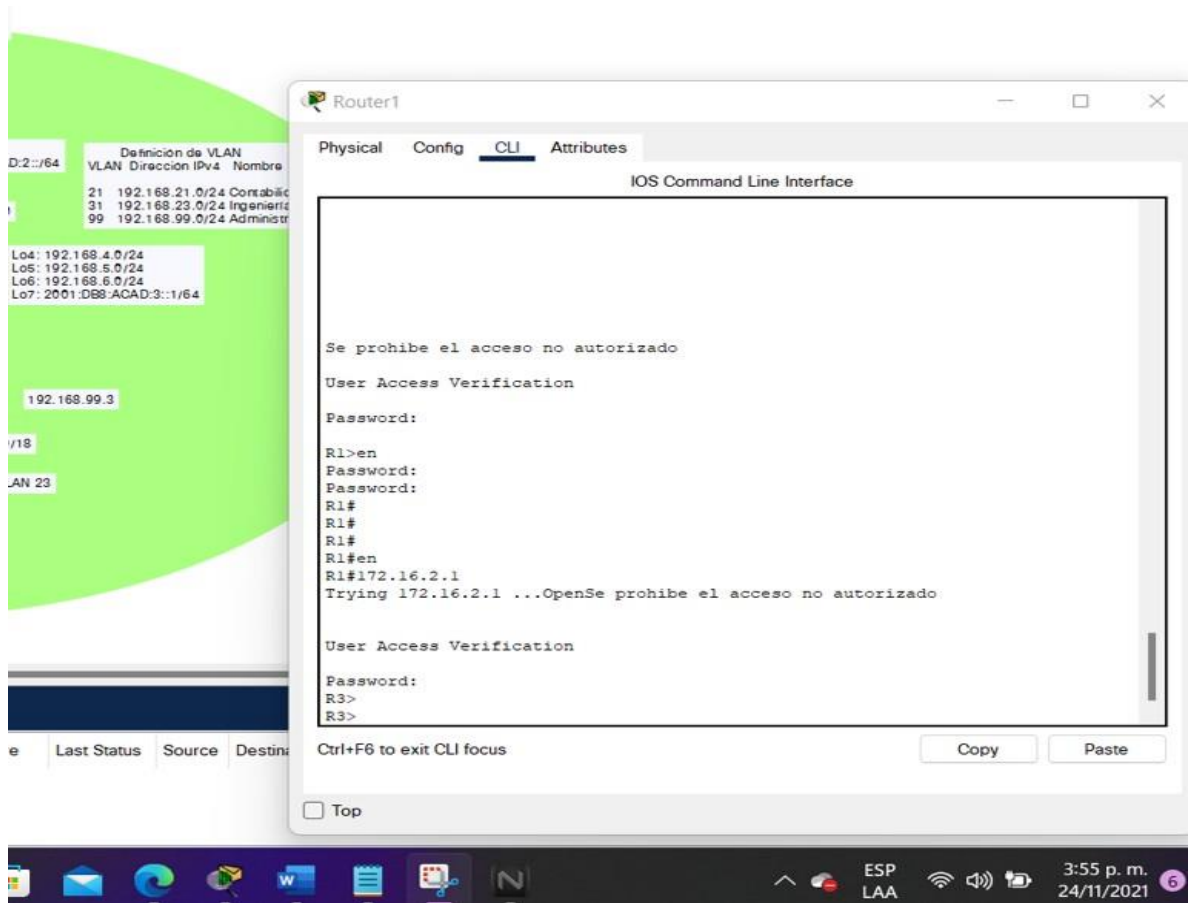
Fuente: Autoría propia

Figura 56. Verificación acceso remoto R1



Fuente: Autoría propia

Figura 57. Verificación acceso remoto a R3



Fuente: Autoría propia

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

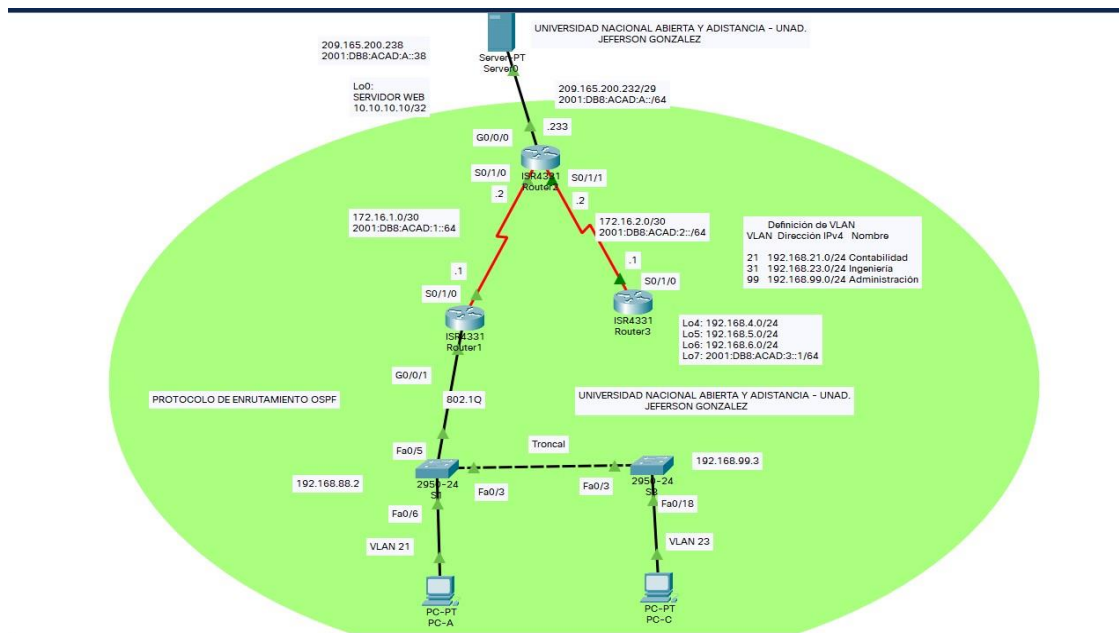
Tabla 26. Comando CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access list
Restablecer los contadores de una lista de acceso	Clear ip Access-list counters

<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<p>R2#sh access-lists</p>
<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <p>R2#sh ip nat st R2#sh ip nat statistics</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>R2#sh ip nat translations R2#clear ip nat translations (no se ejecuta en el ejercicio).</p>

Fuente: Autoría propia

Figura 58. Topología completa escenario



Fuente: Autoría propia

CONCLUSIONES

En este documento, se ha creado dos redes de área local (LAN) que utiliza topología cableada implementado con algunos conceptos importantes como encriptación, creación de usuarios, SSH, creando contraseñas para consola y para modo privilegio, subnetting, vlsm, vlan, utilizando Cisco Packet Tracer. Las dos LAN se han agrupado en una red de 128 y otra de 64 host, utilizando las técnicas ya mencionadas anteriormente, quedando todavía direcciones IP para añadir otras subredes para posible crecimiento en la arquitectura de la red para futuros cambios y configuraciones.

Se realiza configuraciones de routers, switches con diferentes tipos de interfaces, además se logra realizar pruebas de conectividad de cada uno de los routers y switches, con pruebas VLAN, NAT, CLI entre otros comandos especificados en las tablas de tareas.

Se logra realizar la parte de la seguridad del dispositivo, agregando contraseña al modo consola y al modo EXEC privilegiado, encriptación y cifrado de textos, desactivación de búsqueda DNS, además es importante mencionar que se crea un usuario en la base de datos local con su contraseña, se configuran para que solo acepte SSH, se configura la interfaz de administración SVI y se realiza la configuración del Gateway predeterminado de manera correcta logrando el objetivo inicial.

En la ejecución del escenario dos también se logra una verificación sobre las configuraciones de DHCP y NAT estática en la cual se observa que funcionen de forma correcta y sin arrojar errores.

Es importante mencionar que la praxis del software de desarrollo Packet Tracer permitió de forma educativa la configuración de equipos similares al de un aprendizaje de manera física, permitiendo así aprender, ejecutar e incluso cometer errores sin exponer los equipos al daño físico y verificando el tránsito correcto de su comunicación y posible código de error en su configuración, logrando así un gran aprendizaje.

REFERENCIAS BIBLIOGRAFICAS

- [1] BAREÑO, Raul. Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations*. (2021, July). Springer, Cham. (pp. 331-344).
- [2] GUTIERREZ BAREÑO, Raul, NUÑEZ NAVARRO, William, URREA CARDENAS, Sonia, OSORIO SARMIENTO, Hugo, & ACOSTA DUARTE, Nixon. Revisión de la seguridad en la implementación de servicios sobre IPv6. {En línea}. (2016). *Inge Cuc*, 12(1), 86-93. Disponible en https://revistascientificas.cuc.edu.co/ingecuc/article/view/720/pdf_17
- [3] GUTIERREZ BAREÑO, Raul, NUÑEZ NAVARRO, William, URREA CARDENAS, Sonia, OSORIO SARMIENTO, Hugo, & ACOSTA DUARTE, Nixon. Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. {En línea}. (2015). *Revista de Tecnología*, 14(1), 127-138. Disponible en <file:///C:/Users/sansu/Downloads/DialnetAnalisisDeLaSeguridadEnLaImplementacionDeServicios-6041589.pdf>
- [4] GUTIERREZ BAREÑO, Raul, NUÑEZ NAVARRO, William, URREA CARDENAS, Sonia, OSORIO SARMIENTO, Hugo. Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. {En línea}. (2017). *Revista UIS Ingenierías*, 16(1), 75-84. Disponible en <https://revistas.uis.edu.co/index.php/revistausingenierias/article/view/5014/6708>
- [5] GUTIERREZ BAREÑO, Raul. Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco. (2010). Disponible en https://repository.upb.edu.co/bitstream/handle/20.500.11912/1259/digital_20422.pdf?sequence=1&isAllowed=y
- [6] GUTIERREZ BAREÑO, Raul. Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria*. (2017, October). (CONIITI) (pp. 1-5). IEEE.
- [7] MOJICA SANCHEZ, Ivan, GUTIERREZ BAREÑO, Raúl. Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria*. (2019, October). (CONIITI) (pp. 1-6). IEEE.